CYBERCRIME AWARENESS ON SOCIAL MEDIA: A COMPARISON STUDY

Wisdom Umeugo

Independent researcher, Ottawa, Canada

ABSTRACT

The popularity of social media has not waned since it gained popularity in the early 2000s. Social networks such as Facebook, YouTube, Twitter, and Snapchat boast billions of active users worldwide. Social media remains an invaluable tool to both organizations and individuals because of the ease of sharing information and media and the ability to both reach and engage specific audiences of interest. Due to its massive user base, communication ease, and data sharing, social media presents fertile ground for the conduct of cybercrime. Cybercriminals actively target social media users, use social media to facilitate their cybercrime activities, and advertise their criminal activities on social media. The potential dangers of cybercrime on social media necessitate that organizations institute cybercrime on social media policies to guard against these threats and provide employees with cybercrime awareness on social media (CASM) training. CASM is important as corporate and personal use of social media becomes increasingly blurred. This study attempted to measure the CASM scores of employees in security-critical sectors and determine if hearing disability had any impact on the CASM scores. Employees of the education, finance, government, information technology, legal, medicine, military, and Policing sectors in the United States were surveyed. Results showed that the CASM score was average across all sectors. No statistically significant difference in CASM score was found between groups with and without hearing difficulties, although CASM scores were slightly lower for employees with hearing difficulties. The results suggested that more CASM training is needed for employees in the surveyed sectors.

KEYWORDS

Social media, Cybercrime, Cybercrime on social media, Cybercrime awareness,

1. INTRODUCTION

Social media is a phenomenon that has been around for a while. Popular social media platforms like Facebook, YouTube, Snapchat, Instagram, and Twitter need no introduction. Many social media platforms evolved in the early 2000s, revolutionizing how people and businesses communicated and shared information [1], [2]. Social media eased the creation and sharing of diverse media with population segments of interest on their platform [1]. Social media also became the fastest way to grow business enterprises and brands by providing a platform to recruit, disseminate information, advertise, and maintain a branding presence [1]. As a result of its importance and diverse uses, organizations now include social media as part of their competitive strategies [3]–[5]. Organizations use social media for marketing [6], brand awareness [7], customer relationship management [8], reaching buyers across diverse geography [9], recruitment [10], and customer engagement [7]. Private and corporate social media use has become blurry because employees interact with social media as individuals in both professional and personal manners using organizational and personal devices [4].

Despite the popularity and benefits of using social media, the use of social media in both organizational and personal capacities carries risks and dangers. Various threats lurk on social

media that have been identified and classified. Al Hasib [11] organized social networking threats into *privacy-related threats* due to the posting of private information on social media, *information security threats* which are generally known security threats on social media such as worms, viruses, and cross-site scripting, and *identity-related threats* such as phishing, friending malicious actors, profile squatting, stalking, and corporate espionage. Similarly, Fire et al. [12] classified Social media threats into (a) *classic threats,* which are general threats to the internet such as malware, phishing, spammers, fraud, and cross-site scripting; (b) *modern threats* such as clickjacking, fake profile, identity cloning, information leakage, and location leakage that target users' personal information; (c) *combination threats* that combine modern threat methods and classic threat attacks; (d) *attacks targeting children,* such as online predation and cyberbullying. Most of these threats constitute part of larger cybercrimes on social media. Social media is now a medium for all sorts of internet-based crimes, and there is little awareness of these cybercrimes on social media [13]. Social media is also a communication medium for criminal activity due to its speed of information dissemination and short response time [13]. Many known cybercrimes have been highlighted and discussed in the research literature [2], [14]. Notable cybercrimes committed on social media platforms include cyberbullying, hacking, selling illegal things, spreading disinformation, fraud, spam, advertising illegal stuff, and sharing illegal techniques [15].

As with all cybersecurity and cybercrime issues, awareness is critical to help combat cybercrime on social media. Employees and organizations risk falling victim to cybercrime on social media. Awareness is also required to avert inadvertent perpetration and participation in cybercrime on social media. Organizations must incorporate cybercrime on social media awareness into general cybersecurity and cybercrime awareness training. Organizations must also measure their employees' cybercrime on social media awareness levels to gauge the effectiveness of their awareness training programs. Few studies exist on cybercrime awareness on social media, and most cybercrime awareness measurements do not consider cybercrime on social media [16]. Furthermore, none have studied the impact of hearing difficulties on cybercrime awareness on social media. This study attempted to estimate the effects of hearing difficulties on the cybercrime awareness on social media (CASM) of employees in security-critical education, finance, government, information technology, legal, medicine, military, policing, and the STEM sectors. The results of this study will help inform information security managers in security-critical sectors of the need to develop more effective and inclusive CASM programs.

2. LITERATURE REVIEW

Cybercrime is an umbrella term for various illegal acts perpetrated using computer devices and technology systems [17], [18]. Cybercrimes are committed using knowledge of computer systems and cyberspace [19]. Devices used to perpetrate cybercrimes are not limited to computers but also include tablets, smartphones, smart devices, and the Internet of Things (IoT) [16]. Various terms such as online crimes, e-crimes, computer-related crimes, electronic crimes, cybernetic crimes, and digital crimes have been used synonymously to refer to cybercrimes [18]. Cybercrimes can broadly be classified into crimes against digital technologies and crimes that use digital technologies [20]. Anyone with criminal intents and knowledge of cyberspace can perpetrate cybercrimes. Cybercriminals can be script kiddies, cyberterrorists, elite hackers, disgruntled employees, fraudsters, forgers, pirated software vendors, cyber trespassers, and cyberstalkers [16], [18], [21]. Examples of cybercrimes include hacking, distributed denial of service, digital extortion, electronic funds transfer crimes, ATM card fraud, electronic money laundering, tax evasion, offensive material dissemination, information piracy, espionage, cyberbullying, cyberstalking, identity crimes, phishing, spam, cyberterrorism, malware, illegal digital information interception, online obscenity, revenge porn, online hate speech, cyber grooming, and cyber scams [18], [20].

Recently, industry cybercrime reports, government security watchdogs, and academic research works reported a remarkable increase in cybercrime activity during the COVID-19 pandemic. The COVID-19 pandemic ushered in movement restrictions and remote work culture, making technology and cyberspace use critical [22]–[25]. As a result of the dependence on the internet for both domestic and economic activities, the amount of data and activities on the internet surged, causing a corresponding increase in cybercrime activities [24], [26], [27]. Social media, which has long been a popular platform for cybercrime, also saw excessive use during the pandemic [26]–[30]. The excessive use of social media resulted in a surge in social media cybercriminal activities such as phishing, fraud, illegal stuff peddling, and sales of fake medical appliances [26]–[30]. Mass cybercrime awareness campaigns were recommended to combat cybercrimes on social media [27], [31]. Cybercrimes incur costs to individuals, organizations, and society through damages, lost revenues, and defense and mitigation costs [32]. The uptick in cybercrimes is expected to remain in the coming years, costing the world an estimated US$ 10.5 trillion annually by 2025 [33]. The Federal Bureau of Investigation (FBI) estimated that losses to cybercrimes in 2022 amounted to US$ 10.3 Billion [34]. The FBI's Internet crimes complaints center 2022 internet crime report revealed that phishing remained the most reported cybercrime. The 2022 internet crime report also noted that social media was a popular platform and vehicle for phishing, social engineering, data breaches, hacking, and fraudulent crimes [34]. Therefore, individuals, public entities, and enterprises must be aware of cybercrime on social media and have effective defensive strategies.

2.1. Social Media Cybercrimes

Worldwide social media usage has continued to rise. According to [35], 4.76 billion people, or 59% of the people worldwide, actively use social media, and the average time spent per day on social media is about two and a half hours. There was a notable increase in the amount of time spent on social media during the COVID-19 pandemic attributable to lockdown and dependence on internet services [35]. The dangers of using social media are well documented in the research literature. Various research works have extensively discussed the security and privacy [36] threats prevalent on social media [11], [12], [37]. Earlier studies focused on user identity and communication privacy concerns because of the mass sharing of personal information on social media [38]. Other privacy-related threats that arose included inference attacks, information leakage, location leakage, cyberstalking, user profiling, and surveillance [12], [36]. Social media threats evolved with the diversity of social media features, uses, and types of shared media. Fake profiles and identity cloning sprang up for malicious purposes. The widespread use of social media for viral marketing and the installation of third-party applications led to the mass spread of malware, spamming, phishing, social engineering, and clickjacking [36], [39]. Cybercriminals perpetrate all these threats. Fire et al. [12] highlighted the social media crimes against children, such as predation, sharing child pornography, cyberbullying, and cyberharassment.

Cybercrimes on social media can be broadly classified into cybercrimes targeting social media users, cybercrimes facilitated by social media platforms, and cybercrimes advertised on social media platforms [15]. Social media cybercrimes targeted at social media users and their accounts include privacy-violating crimes and account hijacking [15]. Cybercrimes facilitated by social media are classic cybercrimes facilitated through social media. Social engineering, phishing, malware dissemination, scams, fake profiles, account impersonation, cyberstalking, spreading disinformation, spreading hate speech, and cyberharassment are examples of cybercrimes facilitated by social media [15], [37]. Cybercrimes advertised on social media platforms are illegal activities advertised on social media, such as adverts for stolen credit cards, video tutorials of unlawful acts, recruitment for illicit activities, and sharing illegally acquired intellectual property [15], [37].

Humans are considered the weakest link in the cybersecurity protection chain. Similarly, social media users are the weakest link in cybercrime because they not only share private and protected information but are also susceptible to social engineering. Humans also inadvertently participate in the perpetration of cybercrime through social media actions such as likes, sharing, and recommendations [16]. Social media is the favorite platform for executing social engineering and fraud cybercrimes [40]. An estimated 70% of target victims can be found on social media [40].

2.2. Related Work

Various studies have examined and measured cybercrime awareness of specific population demographics. Few have attempted to measure cybercrime on social media awareness, and none have considered deafness and hearing difficulties as a factor. Nzeakor et al. [41] evaluated the pattern of public awareness of cybercrime in Nigeria by surveying 1,031 staff and students of selected tertiary institutions based in Imo State. Nzeakor et al. [41] further analyzed the distribution of cybercrime awareness based on age, sex, and education level. The measured cybercrime awareness level was high. Males in the study had higher awareness than females. Higher levels of education were found to correlate with higher awareness levels.

Karagiannopoulos et al. [42] investigated the cybercrime awareness of individuals over 60 years. Karagiannopoulos et al. [42] noted that people over 60 were more prone to cybercrime victimization and that existing cybercrime awareness education could have been more helpful to them. Karagiannopoulos et al. [42] conducted a semi-structured interview with fifteen adults over 60. Awareness levels varied among the participants, and most participants had been previous victims of cybercrime. Karagiannopoulos et al. [42] concluded that social media awareness training must be tailored for people over 60. Although participants in the study were social media users, most used their social media accounts to interact with younger relatives. Karagiannopoulos et al. [42] provided no quantitative awareness level information.

Nzeakor et al. [43] examined the current trend in cybercrime awareness of 1104 internet users in Umuahia, Abia State, Nigeria, using a questionnaire supplemented with an in-depth interview. Nzeakor et al. [43] found that cybercrime awareness was high because two-thirds of participants demonstrated adequate cybercrime awareness. Awareness of fraud-related cybercrimes, e-theft, hacking, and ATM theft was more heightened in participants than awareness of sexually-related offenses, cyber-terrorism, identity theft, spam, and malware attacks.

Zayid and Farah [44] studied the cybercrime risks and awareness levels of Bisha University College Science and Arts students in the Al-Namas district in southern Saudi Arabia. Their study surveyed 135 randomly chosen students using an open-ended questionnaire. Results showed that students' cybercrime awareness levels were weak because only 8.9% of the participants had excellent cybercrime awareness. The study also found that social media was the most used platform for delivering malware.

Ismailova and Muhametjanova [45] evaluated students' cybercrime risk awareness in the Kyrgyz Republic. A survey of 172 students revealed low cybercrime awareness among students. Ismailova and Muhametjanova [45] further analyzed the relationship between the computer literacy rate and cybercrime risk awareness levels. ANOVA test results on the data showed that the cybercrime risk awareness levels significantly differed between students with low and high computer literacy levels.

Irshad and Soomro [46] explored how identity theft was executed on social media. Their study included a short survey containing ten questions related to social media usage and social media cybercrime awareness. The survey was administered to 104 respondents worldwide. The results

showed that 88% of respondents knew that social media was used to commit cybercrime. Respondents also identified cyberstalking, cyberbullying, and identity theft as the most severe social media cybercrime.

Prior studies have demonstrated that awareness is an important cybercrime preventive measure [13], [47], [48]. Awareness of cybercrimes on social media is, therefore, equally important. No research has attempted to measure cybercrime on social media awareness using a validated scale. Quantitative scales such as the Human Aspects of Information Security Questionnaire (HAIS-Q) [49] and the security behavior intention scale (SeBIS) [50] have been developed and used in measuring information security awareness and security behavior intention, respectively. Arpaci and Aslan [16] created a validated cybercrime awareness on social media scale (CASM-S) to measure CASM directly. CASM-S is unidimensional and consists of 22 items rated on a five-point Likert scale. No items in CASM-S are reverse-coded. CASM-S was the adopted scale for this study.

3. RESEARCH QUESTIONS

Four research questions were formulated to guide this study:

Research Question One: What are the overall CASM scores for all employees combined?
H1: All employees combined have a good CASM score.

Research Question Two: What are the estimated CASM scores by employment sectors?
H2: Employees in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors all have good CASM scores.

Research Question Three: What are the estimated CASM scores of employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors?
H3: Employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors have good CASM scores.

Research Question Four: Is there a statistically significant difference between the estimated CASM scores of employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors?
H4: There is no statistically significant difference between the estimated CASM scores of employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors.

4. RESEARCH METHOD

The study administered an online survey to a random sample of Prolific adult audience working full-time in the education, finance, government, information technology, legal, medicine, military, policing, and STEM sectors in the United States. G*Power was used to calculate a minimum sample size of 210 for ANOVA fixed effects, omnibus, one-way test at 0.25 effect size, 0.05 error probability, 0.95 power, and two groups. CASM was measured using the CASM-S scale developed by [16]. The CASM-S survey was closed-ended and consisted of 22 five-point Likert scale variable measurement questions. The Likert scale measurement used was Strongly disagree (1) to Strongly agree (5). Social desirability bias was reduced in the study by informing

participants that their responses would remain anonymous. Participants were also asked to answer the questions truthfully. A total of 386 valid responses were accepted after data quality checks. The data was imported into Jamovi for statistical analysis. CASM scores were calculated and expressed as a percentage of the maximum achievable score. The interpretation scale by [51] was used where a score of 80%-100% was considered good, 60%-79% average, and 59% and less interpreted as poor awareness. The high score requirement for a good awareness level was due to the high-security requirements of the surveyed sectors.

5. RESULTS

Out of the 386 respondents, there were 254 males and 132 females. Most of the participants were aged between 25 and 34 years old. 147 or 38.1% of the participants had hearing difficulties, while 239 participants (61.9%) reported having no hearing difficulties. Table 1 summarizes the study's participant demographics. The questionnaire reliability was assessed using Cronbach alpha. The questionnaire showed high reliability with a Cronbach alpha score of 0.905.

Table 1. Participant Demographics

Demographic	Category	Frequency (n)	Percent (%)
sex	Female	132	34.2
	Male	254	65.8
age	18-24	24	6.2
	25-34	148	38.3
	34-44	105	27.2
	44-54	72	18.7
	54 and above	37	9.6
Education	Doctorate	30	7.8
	Graduate degree	96	24.9
	High school diploma	29	7.5
	Secondary education	1	0.3
	Technical/community college	43	11.1
	Undergraduate degree	187	48.4
Employment sector	Education & Training	74	19.2
	Finance	49	12.7
	Government & Public Administration	39	10.1
	Information Technology	82	21.2
	Legal	10	2.6
	Medicine	72	18.7
	Military	3	0.8
	Policing	2	0.5
	Science, Technology, Engineering & Mathematics	55	14.2
Hearing difficulties	No	239	61.9
	Yes	147	38.1

5.1. Research Question One

To answer Research question one, the scores were calculated as a percentage of the maximum score and the mean taken. The mean CASM score of all participants was 69.6%, an average score. Hypothesis H1 stating that all employees combined have a good CASM score, was rejected.

5.2. Research Question Two

All employment sectors had average CASM scores except the military sector, which had a poor CASM score. The policing sector had the highest CASM score of 73.6% but had only two participants. A participant from the medicine sector had the lowest CASM score of 34.5%. Participants in the legal, education & training, and finance sectors had the next highest CASM scores of 72.6%, 71.9%, and 71%, respectively. The Military sector had the lowest CASM score of 49.7%. Table. 2 summarizes the CASM score by employment sector. Figure 1 depicts the employment sector CASM scores graphically. Hypothesis H2, stating that employees in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors all have good CASM scores, was therefore rejected.

Table 2. Employment Sector CASM Scores

Employment sector	N	CASM Score (%)
Education & Training	74	71.9
Finance	49	71.1
Government & Public Administration	39	67.9
Information Technology	82	67.1
Legal	10	72.6
Medicine	72	69.8
Military	3	49.7
Policing	2	73.6
Science, Technology, Engineering & Mathematics	55	69.9

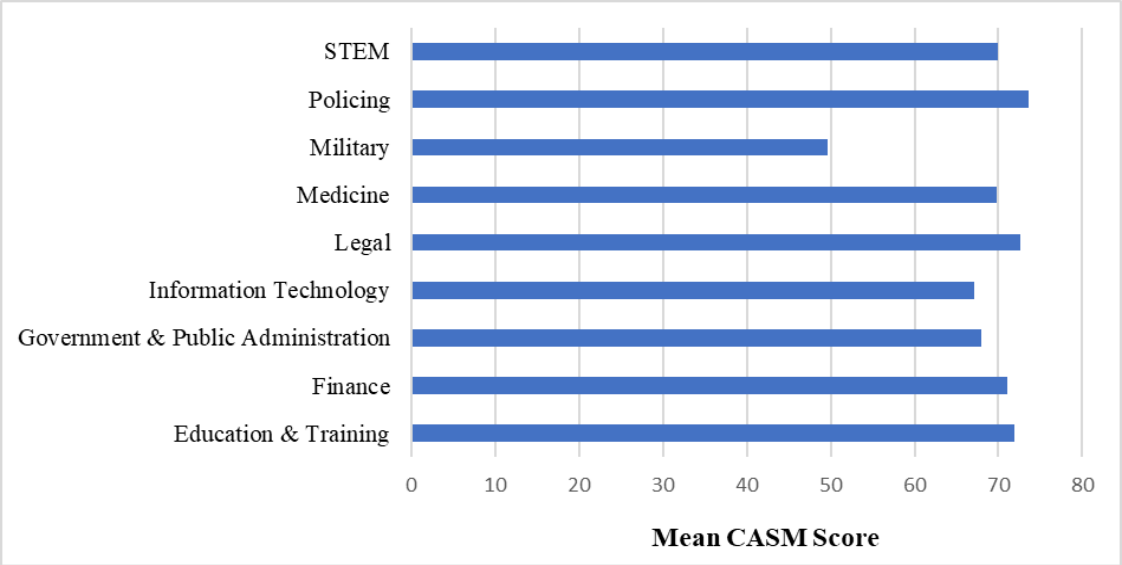

Figure 1. CASM Score by employment sector.

5.3. Research Question Three

The CASM score for each hearing difficulty group was calculated. Both groups had scores in the average range. The CASM score for participants with no hearing difficulties was 70.4%, slightly

higher than the 68.1% CASM score for participants with hearing difficulties. Table 3 shows the CASM scores for the hearing difficulties groups.

Table 3. Hearing Difficulties Group CASM Scores

Hearing difficulties	N	CASM Score
No	239	70.4
Yes	147	68.1

The hearing difficulties group mean CASM scores distributed across each employment sector are shown in Table 4. The CASM score was higher for participants with no hearing difficulties in the education & training, finance, government & public administration, military, and STEM employment sectors. The CASM scores of participants with hearing difficulties were higher than participants with no hearing difficulties in the legal, medicine, and policing employment sectors. The most significant difference between the two hearing difficulties groups was in the policing (45%) and legal (11%) employment sectors. Based on the result, Hypothesis H3 stating that employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors have good CASM scores, was rejected. Figure 2 graphically depicts the CASM scores of hearing difficulty groups across employment sectors.

Table 4. Hearing difficulties group mean CASM across employment sectors.

Hearing difficulties	Employment sector	N	CASM Score
No	Education & Training	45	74.9
	Finance	30	73.8
	Government & Public Administration	20	68.3
	Information Technology	56	68.0
	Legal	7	69.3
	Medicine	36	69.2
	Military	2	50.5
	Policing	1	50.9
	STEM	42	70.2
Yes	Education & Training	29	67.1
	Finance	19	66.9
	Government & Public Administration	19	67.6
	Information Technology	26	65.2
	Legal	3	80.3
	Medicine	36	70.5
	Military	1	48.2
	Policing	1	96.4
	STEM	13	69.0

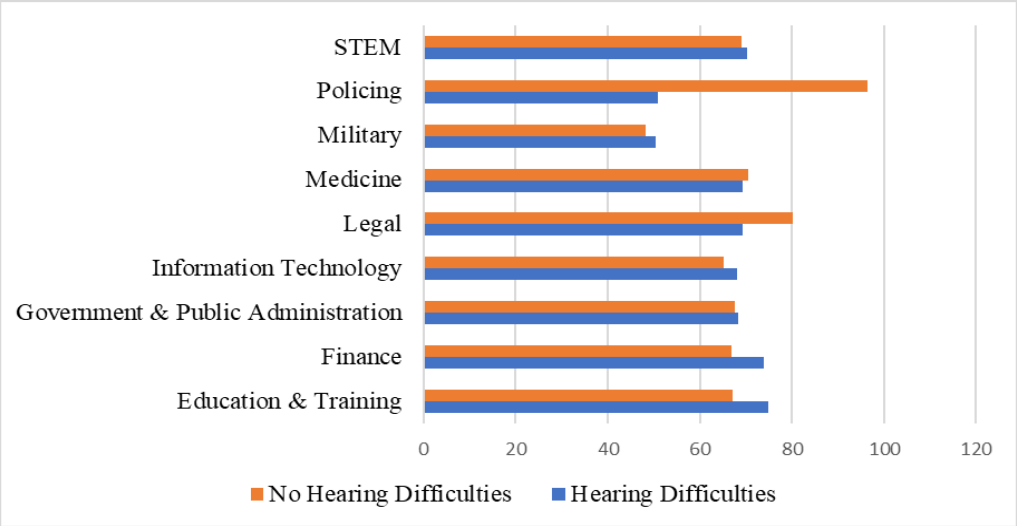

Figure 2. CASM scores of hearing difficulty groups across employment sectors

5.4. Research Question Four

An ANOVA analysis was performed on the data to answer research question four. The dependent variable was the hearing difficulties group mean CASM across employment sectors, while the independent variable was hearing difficulties with its two categories. Shapiro-Wilk and Levene's tests were used to check the data for linearity and homogeneity of the variance, respectively. The data failed the ANOVA linearity test with statistically significant Shapiro-wilk test results, as shown in Table 4. The data passed Levene's test for homogeneity of variance with statistically insignificant p-values, as shown in Table 5.

Table 5. Shapiro-Wilk Test Score

	Statistic	**p**
Shapiro-Wilk	0.988	0.002

Table 6. Levene's Test Result

	Statistic	**df**	**df2**	**p**
Levene's	0.996	1	384	0.319

The Kruskal-Wallis test was conducted instead of ANOVA because the data failed the ANOVA linearity assumption. Table 6 shows the result of the Kruskal-Wallis test for the difference in mean between the hearing difficulty groups. There were no statistically significant differences between groups of hearing difficulty for CASM score ($\chi 2$ (1) = 1.98, p =.159). Therefore, there is no significant difference between the estimated CASM scores of people with and without hearing difficulties working in the education, finance, government, information technology, legal, medicine, military, policing, and STEM employment sectors. Hypothesis H4 stating that there is no statistically significant difference between the estimated CASM scores of employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors, was retained based on the Kruskal-Wallis test result.

Table 7. Kruskal-Wallis Test Result

	χ^2	df	p
Kruskal-Wallis	1.98	1	0.159

5.5. Summary of Hypotheses Tests

Based on the results, Hypotheses H1, H2, and H3 were all rejected because CASM scores were mostly average. Hypothesis H4 was retained, supported by the statistically insignificant Kruskal-Wallis test result. Table 8 summarizes the result of the hypotheses test.

Table 8. Hypotheses testing results.

Hypothesis	Result
H1: All employees combined have a good CASM score.	Rejected
H2: Employees in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors all have good CASM scores.	Rejected
H3: Employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors have good CASM scores.	Rejected
H4: There is no statistically significant difference between the estimated CASM scores of employees with and without hearing difficulties working in the education, finance, information technology, legal, military, medicine, policing, government, and STEM sectors.	Retained

6. DISCUSSION

All participants' mean CASM score was 69.6%, an average score. Security-critical employment sectors like those surveyed should have above-average CASM scores. The results point to a need for more CASM training. The CASM score for the military sector was poor at 49.7%. Although the Military was underrepresented in the study, with as few as three participants, the score is very worrying. Even the equally underrepresented policing employment sector, with just two participants, had a much better CASM score of 73.6%. Hearing difficulties made little difference in the CASM scores of the surveyed participants. The difference in the mean CASM scores between the hearing difficulties group was approximately 2%. This little difference may imply that organizations in the surveyed employment sectors, on average, provide some form of CASM awareness training. The observed differences between the scores of the two hearing difficulties groups were also not statistically significant, as determined by the Kruskal-Wallis test result. When the hearing difficulties group scores are viewed by the employment sector, the scores of participants with hearing difficulties are mostly lower than those without. The legal, policing, and medicine employment sectors had higher CASM scores for participants with hearing difficulty. However, the sample sizes for the two groups in the legal, policing, and medicine sectors were closely identical, which may have contributed to the higher scores for the group with hearing difficulties in these three sectors.

7. LIMITATIONS

This study has several limitations. The study's population was limited to employees in the surveyed sectors, and the sample size does not fully represent the population of employees across the surveyed sectors. The military and policing employment sectors were also underrepresented

in the study. The study did not consider the different hearing difficulty levels in its analysis. The study was also limited to the United States, limiting results generalization across countries.

8. CONCLUSION

Human factors have long been considered the weakest link in information security. Social media is often used for malicious information gathering and attacks. Social media's popularity and high usage make it a highly effective platform for cybercrime. Employers must educate their employees on the potential dangers lurking in social media and provide policies governing what organizational information employees post. This study measured employees' cybercrime awareness on social media (CASM) in the Information technology, STEM, military, policing, legal, medicine, government & public administration, and education & training sectors. Employees of these sectors were surveyed for their self-reported CASM scores. The calculated CASM score across all sectors was average. Organizations in the surveyed sectors need to provide their employees with more cybercrime awareness on social media training. The lack of statistically significant difference in the CASM scores of groups with and without hearing difficulties may point to the fact that either there is no CASM awareness training among employees in the surveyed sectors or that the CASM training given, if any, has similar average impact across the two hearing difficulty groups. More studies are needed on the direct effects of CASM training on the two hearing difficulties groups across multiple employment sectors.

REFERENCES

[1] S. Edosomwan, S. K. Prakasan, D. Kouame, J. Watson, and T. Seymour, "The history of social media and its impact on business.," Journal of Applied Management and entrepreneurship, vol. 16, no. 3, 2011.

[2] L. Almadhoor, "Social media and cybercrimes.," Turkish Journal of Computer and Mathematics Education (TURCOMAT), vol. 12, no. 10, pp. 2972–2981, 2021.

[3] H. J. Wilson, P. J. Guinan, S. Parise, and B. D. Weinberg, "What's your social media strategy?," IEEE Eng. Manag. Rev., vol. 41, no. 3, pp. 14–16, 2013, doi: 10.1109/EMR.2013.6596542.

[4] R. Effing, "Social media strategy design.," presented at the 2nd Scientific Conference Information Science in an Age of Change, Insitute of Information and Book Studies, University of Warsaw, Warsaw, Apr. 2013.

[5] N. Tourani, "Thriving in a shifting landscape: Role of social media in support of business strategy," Asia Pacific Management Review, vol. 27, no. 4, pp. 276–281, Dec. 2022, doi: 10.1016/j.apmrv.2021.11.001.

[6] E. S. Soegoto and A. T. Utomo, "Marketing strategy through social media," IOP Conf. Ser.: Mater. Sci. Eng., vol. 662, no. 3, p. 032040, Nov. 2019, doi: 10.1088/1757-899X/662/3/032040.

[7] G. Tsimonis and S. Dimitriadis, "Brand strategies in social media," Mrkting Intelligence & Plan, vol. 32, no. 3, pp. 328–344, Apr. 2014, doi: 10.1108/MIP-04-2013-0056.

[8] C. A. Elena, "Social media – A strategy in developing customer relationship management," Procedia Economics and Finance, vol. 39, pp. 785–790, 2016, doi: 10.1016/S2212-5671(16)30266-0.

[9] H. Gao, M. Tate, H. Zhang, S. Chen, and B. Liang, "Social Media Ties Strategy in International Branding: An Application of Resource-Based Theory," Journal of International Marketing, vol. 26, no. 3, p. jim.17.0014, May 2018, doi: 10.1509/jim.17.0014.

[10] S. A. Madia, "Best practices for using social media as a recruitment strategy," Strategic HR Review, vol. 10, no. 6, pp. 19–24, Oct. 2011, doi: 10.1108/14754391111172788.

[11] A. Al Hasib, "Threats of online social networks.," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 11, pp. 288–93, 2009.

[12] M. Fire, R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," IEEE Commun. Surv. Tutorials, vol. 16, no. 4, pp. 2019–2036, 2014, doi: 10.1109/COMST.2014.2321628.

[13] T. R. Soomro and M. Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," Applied Computer Systems, vol. 24, no. 1, pp. 9–17, May 2019, doi: 10.2478/acss-2019-0002.

[14] S. Sharma and V. K. Sharma, "Cyber Crime analysis on Social Media," BJOC, May 2020, doi: 10.51767/jc1104.
[15] Reliaquest, "How Cybercriminals Weaponize Social Media - ReliaQuest," Reliaquest, Aug. 25, 2021. https://www.reliaquest.com/blog/how-cybercriminals-weaponize-social-media/ (accessed Mar. 05, 2023).
[16] I. Arpaci and O. Aslan, "Development of a Scale to Measure Cybercrime-Awareness on Social Media," Journal of Computer Information Systems, pp. 1–11, Jul. 2022, doi: 10.1080/08874417.2022.2101160.
[17] A. M. Bossler and T. Berenblum, "Introduction: new directions in cybercrime research," Journal of Crime and Justice, vol. 42, no. 5, pp. 495–499, Oct. 2019, doi: 10.1080/0735648X.2019.1692426.
[18] R. Sabillon, J. J. Cano, V. C. Reyes, and J. S. Ruiz, "Cybercrime and cybercriminals: A comprehensive study.," International Journal of Computer Networks and Communications Security, 2016, 4 (6), 2016.
[19] S. Furnell, "Cybercrime: vandalizing the information society," in Web Engineering, vol. 2722, J. M. C. Lovelle, B. M. G. Rodríguez, J. E. L. Gayo, M. del Puerto Paule Ruiz, and L. J. Aguilar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 8–16.
[20] P. Grabosky and R. Smith, "Cybercrime.," Crime and Justice: A Guide to Criminology (4th ed), 2012.
[21] S. Gordon and R. Ford, "On the definition and classification of cybercrime," J. Comput. Virol., vol. 2, no. 1, pp. 13–20, Aug. 2006, doi: 10.1007/s11416-006-0015-z.
[22] Council of Europe, "Cybercrime and COVID-19 - Cybercrime," Mar. 27, 2020. https://www.coe.int/en/web/cybercrime/news/-/asset_publisher/S73WWxscOuZ5/content/cybercrime-and-covid-19 (accessed Mar. 14, 2023).
[23] INTERPOL, "INTERPOL report shows alarming rate of cyberattacks during COVID-19," Aug. 04, 2020. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (accessed Mar. 14, 2023).
[24] A. Radoini, "Cyber-crime during the COVID-19 pandemic," Freedom from Fear, vol. 2020, no. 16, pp. 6–10, Oct. 2020, doi: 10.18356/5c95a747-en.
[25] M. Plachkinova, "Exploring the Shift from Physical to Cybercrime at the Onset of the COVID-19 Pandemic," CFATI, vol. 2, no. 1, pp. 50–62, May 2021, doi: 10.46386/ijcfati.v2i1.29.
[26] M. Kashif, M. K. Javed, and D. Pandey, "A surge in cyber-crime during COVID-19.," Indonesian Journal of Social and Environmental Issues (IJSEI), vol. 1, no. 2, pp. 48–52, 2020.
[27] A. Gryszczyńska, "The impact of the COVID-19 pandemic on cybercrime.," Bulletin of the Polish Academy of Sciences: Technical Sciences, 2021.
[28] B. Collier, S. Horgan, R. Jones, and L. Shepherd, "The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations.," Scottish Institute for Policing Research, 2020.
[29] A. H. Amarullah, A. J. S. Runturambi, and B. Widiawan, "Analyzing Cyber Crimes during COVID-19 Time in Indonesia," in 2021 3rd International Conference on Computer Communication and the Internet (ICCCI), Jun. 2021, pp. 78–83, doi: 10.1109/ICCCI51764.2021.9486775.
[30] I. Arpaci, K. Karatas, F. Kiran, I. Kusci, and A. Topcu, "Mediating role of positivity in the relationship between state anxiety and problematic social media use during the COVID-19 pandemic.," Death Stud., vol. 46, no. 10, pp. 2287–2297, 2022, doi: 10.1080/07481187.2021.1923588.
[31] B. Pranggono and A. Arabo, "COVID -19 pandemic cybersecurity issues," Internet Technology Letters, vol. 4, no. 2, Mar. 2021, doi: 10.1002/itl2.247.
[32] R. Anderson et al., "Measuring the cost of cybercrime," in The economics of information security and privacy, R. Böhme, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 265–300.
[33] S. Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Cybercrime Magazine, Nov. 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed Mar. 15, 2023).
[34] Internet Crime Complaint Center, "FEDERAL BUREAU of INVESTIGATION Internet Crime report 2022," 2022, Accessed: Mar. 13, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
[35] D. Chaffey, "Global social media statistics research summary 2023," Smart Insights, Jan. 30, 2023. https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/ (accessed Mar. 14, 2023).

[36] S. Ali, N. Islam, A. Rauf, I. Din, M. Guizani, and J. Rodrigues, "Privacy and security issues in online social networks," Future Internet, vol. 10, no. 12, p. 114, Nov. 2018, doi: 10.3390/fi10120114.
[37] M. B. Yassein, S. Aljawarneh, and Y. A. Wahsheh, "Survey of online social networks threats and solutions," in 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Apr. 2019, pp. 375–380, doi: 10.1109/JEEIT.2019.8717381.
[38] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," IEEE Netw., vol. 24, no. 4, pp. 13–18, 2010, doi: 10.1109/MNET.2010.5510913.
[39] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, "Security issues in online social networks," IEEE Internet Comput., vol. 15, no. 4, pp. 56–63, Jul. 2011, doi: 10.1109/MIC.2011.50.
[40] Graphus, "Phishing Scammers Have Flocked to Social Media ," Feb. 17, 2022. https://www.graphus.ai/blog/phishing-scammers-have-flocked-to-social-media/ (accessed Mar. 15, 2023).
[41] O. F. Nzeakor, B. N. Nwokeoma, and P. J. Ezeh, "Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment.," International Journal of Cyber Criminology, vol. 14, no. 1, pp. 283–299, 2020.
[42] Dr. V. Karagiannopoulos, Dr. A. Kirby, S. Oftadeh-Moghadam, and Dr. L. Sugiura, "Cybercrime awareness and victimisation in individuals over 60 years: A Portsmouth case study," Computer Law & Security Review, vol. 43, p. 105615, Nov. 2021, doi: 10.1016/j.clsr.2021.105615.
[43] O. F. Nzeakor, B. N. Nwokeoma, I. Hassan, O. B. Ajah, and J. T. Okpa, "Emerging trends in cybercrime awareness in Nigeria.," International Journal of Cybersecurity Intelligence & Cybercrime, vol. 5, no. 3, pp. 41–67, 2022.
[44] E. I. M. Zayid and N. A. A. Farah, "A study on cybercrime awareness test in Saudi Arabia - Alnamas region," in 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Mar. 2017, pp. 199–202, doi: 10.1109/Anti-Cybercrime.2017.7905290.
[45] R. Ismailova and G. Muhametjanova, "Cyber crime risk awareness in Kyrgyz Republic," Information Security Journal: A Global Perspective, vol. 25, no. 1–3, pp. 32–38, Apr. 2016, doi: 10.1080/19393555.2015.1132800.
[46] S. Irshad and T. R. Soomro, "Identity theft and social media.," International Journal of Computer Science and Network Security, vol. 18, no. 1, pp. 43–55, 2018.
[47] L. Buono, "Fighting cybercrime through prevention, outreach and awareness raising," ERA Forum, vol. 15, no. 1, pp. 1–8, Jun. 2014, doi: 10.1007/s12027-014-0333-4.
[48] J. L. Bele, M. Dimc, D. Rozman, and A. S. Jemec, Raising Awareness of Cybercrime--The Use of Education as a Means of Prevention and Protection. International Association for the Development of the Information Society, 2014.
[49] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," Computers & Security, vol. 42, pp. 165–176, May 2014, doi: 10.1016/j.cose.2013.12.003.
[50] S. Egelman and E. Peer, "Scaling the security wall: developing a security behavior intentions scale (sebis)," in Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems - CHI '15, New York, New York, USA, Apr. 2015, pp. 2873–2882, doi: 10.1145/2702123.2702249.
[51] K. F. Arisya, Y. Ruldeviyani, R. Prakoso, and A. L. Fadhilah, "Measurement of information security awareness level: A case study of mobile banking (m-banking) users.," 2020 Fifth International Conference On Informatics And Computing (Icic), p. 1, 2020.