International Journal of Applied and Scientific Research (IJASR)
Vol. 3, No. 1, 2025 : 67-82

Cybersecurity Awareness in Higher Education: Evaluating the Impact of Online Safety Campaigns

Macliffton Tembak Sinau[1]*, Niza Wahida binti Wahishad[2]
[1] Institute of Teacher Education, Tun Abdul Razak Campus
[2]Nanga Merit Primary School

Corresponding Author: Macliffton Tembak Sinau cikgumike0203@gmail.com

A R T I C L E I N F O

Keywords: Online Safety Awareness, Risky Online Behavior, Cybersecurity Education, Online Privacy, Cybercrime Prevention, Internet Security

Received : 5 November
Revised : 23 December
Accepted: 23 January

A B S T R A C T

The rise of digital technologies has increased university students' exposure to cyber risks, highlighting the need for effective online safety campaigns. This study examines their impact on reducing risky online behaviors using a quantitative survey. Findings show that targeted awareness programs improve cybersecurity knowledge, reducing unsafe activities like sharing personal information, falling for phishing scams, and weak password use. Frequent exposure to cybersecurity education fosters responsible digital behavior, emphasizing the need to integrate online safety programs into university curricula. Additionally, adaptive and interactive training methods are essential for long-term behavioral change. This study contributes to cybercrime prevention by providing insights into the effectiveness of digital safety education for young adults

DOI: https://doi.org/10.59890/ijasr.v3i1.459
ISSN-E: 3025-7670
https://journal.multitechpublisher.com/index.php/ijasr/

INTRODUCTION

Online safety awareness campaigns serve as a crucial attempt to help significantly reduce the increasing rise of risky behaviors in the vast online world that we navigate today. As the internet continues to become a more integral part of our lives, there is an alarming increase in the number of crimes and vulnerabilities associated with online applications. These online criminal acts are not only instigated by skilled hackers but are also, quite alarmingly, perpetrated by individuals who may be acting entirely unintentionally, all due to a lack of awareness regarding online safety (Ayyoub et al., 2022). Therefore, robust safety awareness is not just beneficial; it is essential to avoid these vulnerabilities and notably reduce the likelihood of being targeted by perpetrators of online crime, thus fostering a more secure digital experience.

The online world should inherently offer many advantages, primarily due to the easy access it provides to a vast array of useful and informative material. However, on the other side of the coin, the internet also harbors numerous potential risks and dangers, which may include harmful viruses, relentless spam, various forms of fraud, and other inappropriate material that can be detrimental to users. The implementation of well-structured student internet use policies on university campuses is of paramount importance, as it could significantly enhance their knowledge and contribute positively to their academic performance (Chowdhury, 2024). There exists a wide range of educational materials available that can be utilized to enrich their understanding and learning experiences. However, the ease of accessing this material can also lead to potential negative consequences. There is a real concern regarding university students possibly becoming overly obsessed with the internet, which can lead to them spending excessive amounts of time online while accessing material that may not be appropriate or beneficial for them (Shabahang et al., 2021). This phenomenon could result in adverse effects, including a reduction in the quality of their learning processes, the isolation of students from their real-world communities, and even escalating into risky situations within the online sphere.

This study specifically focuses on the implementation and effectiveness of the online safety awareness campaign targeted toward university students. In the unique context of Malaysian, these individuals are at a critical emotional stage in their lives and require guidance to develop their awareness surrounding online safety. Consequently, this study concentrates solely on university students as the primary subject of the research rather than seeking to address a broader audience. The primary aim of this research is to assess the effectiveness of an online safety awareness campaign aimed at university students, with the overarching goal of mitigating their risky behavior in the online world.

An online safety awareness campaign represents a dedicated effort to maintain a safe online environment for all users. A safer online environment is characterized by conditions in which individuals can engage without fear of harassment or exposure to dangerous activities. For this reason, online safety awareness campaigns should be conducted continuously to ensure that a safe online environment can be maintained (Admass et al., 2024). These campaigns serve a vital role as they encourage individuals to think more critically about their

online actions and the materials they encounter. However, despite their importance, these sorts of campaigns are urgently needed because the online environment is constantly evolving, and new risks continuously emerge, presenting themselves to unsuspecting users. Ideally, with the proper awareness instilled in users, individuals should be able to recognize the risks they face and understand the ways to combat them effectively (Mensah, 2023). Nevertheless, it is critical to acknowledge that social engineering attacks remain effective because, by design, they exploit vulnerable spots in human behavior and digital practices.

LITERATURE REVIEW

The advent of the Internet has brought numerous changes to our daily lives. A large part of our communication, knowledge, and social interaction is now taking place online. One of the most significant alterations is in the realm of knowledge exchange. Many users look for information online, which has further granted significance for any policies or campaigns related to this domain (Khaund et al., 2021). Many of these users are university students who often form a substantial proportion of a country's population and represent an important part of its future. Recent studies show that problematic Internet use has health side effects besides reducing study time and causing stressful lives. Since university students often quit parental surveillance and are exposed to a high degree of stress due to their educational requirements, they need to be the target of many online safety awareness campaigns (Teimouri et al., 2018).

Therefore, the importance of exploring the effectiveness of various campaign factors in enhancing their positive effects is inevitable. This is especially true for negative use of the Internet, e.g. watching offensive sexual content on the Internet. Such campaigns refer to any organized, planned events – online or offline – that are aimed to enhance individuals' knowledge about online risks and learn how to protect oneself from different kinds of online dangers. The range of online safety awareness campaigns is plentiful. In the literature one may come across terms from basic education or actions within special projects that focus on IT security (Nifakos et al., 2021). Sometimes a wider approach is taken and within its framework ISPs and the private sector provide free of charge filtering and monitoring software for the citizen. In the globalized world there are public-private partnerships that are aimed to promote online safety.

Cyber crimes and risky online behaviors are significant social issues in contemporary information societies. They endanger the security and well-being of individuals and communities. Statistics reveal that crimes like cyberbullying, online fraud, illicit downloading, and Internet addiction are prevalent among young groups and particularly university students. Treatment and prevention of such phenomena and the promotion of a safe online environment requires transdisciplinary examination from the fields of psychology, sociology, legislation, and technology (Schulte et al., 2022). In particular, it may be effective to test the extent to which university students know their legal rights, understand the psychosocial impacts of being a victimizer or a victim of cybercrimes, are

experienced with protective digital technologies, and become aware of the norms, culture, and limitations in the use of digitalized media and communication channels.

So far, no studies have been conducted that reveal a concise and accurate awareness and protection from online crimes and risky behaviors and the psychosocial phenomena behind this response. Consequently, nurturing such knowledge and skills may be a positive step in preventing and reducing Internet-added and cybercriminal behavior (Teimouri et al., 2018). Efforts to promote information security should not solely focus on enhancing the individual-level cognitions of Internet users toward cyber security. It is important to take a multidisciplinary approach that examines the role played by factors at the psychological, social, and technological levels. By examining these issues, insights can be gained that have the potential to inform educational interventions delivered by educational institutions to promote safer online behaviors. A cognitive-affective model of risky online behavior is proposed drawing on aspects of the Theory of Planned Behavior and Protection Motivation Theory that highlights the influence of risk cognitions and promoting the adoption of protective behaviors in the context of online safety (Foroutan et al., 2022).

Theoretical Framework

Theoretical Background In order to gain a greater understanding of such behavior, investigations have taken place regarding additional factors that may also affect what could be considered the highest priority risks. This would find its complete level of expression on the internet and digital communications – the primary concern of parents and universities with responsibility for safeguarding minors. A policy-based literature review has been carried out to discover, among other things, the focus of research and, possibly, the distraction from what is empirically an even greater threat. It is postulated, putting aside such immediate dangers, that the focus of successful research works appears to contravene the primacy of social weight, seeking risks instead where cognitive ability of minors is even less developed. This would suggest that the form attention is being paid to the children which implies a particular viewpoint with regards to each topic area. This approach may therefore be deficient; not sufficiently considering the differences between children's perception of activities and that of some adults who investigate them.

Relevant Theories There exists a diverse array of multiple models and theories that may be instrumental in unlocking various elements concerning how risky online behavior may be interconnected. In numerous aspects of this field, these theories can indeed be categorized in broadly similar frameworks (Flayelle et al., 2023). For instance, on the internet, it is essential to understand that what is expressed is not always indicative of what is genuinely meant or felt by the individual; this discrepancy is largely due to the significant absence of non-verbal cues, which can make the true behavioral intentions challenging to discern effectively. Nonetheless, such intentions and emotions are frequently communicated online, albeit in different ways. Moreover, throwaway comments, which may be perceived as trivial, can often be typed with more ease than they

would be spoken in face-to-face interactions (Peterson & Husu, 2023). This phenomenon further complicates the understanding of online behavior.

Knowledge The concept of university students knowing about online safety is not such a recent one in the literature (Zwilling et al., 2022). Indeed, that knowledge is a crucial antecedent to the encouragement of safe behavior is known to have its roots as long ago as the 1950s. Knowledge is an essential component in biology and cognitive psychology with vast numbers of disciplines recognizing that a lack of such hinders recognition and response to risks. This would suggest, as in a logical extension, that to prevent harm from internet use minors ought to know how to harm could occur (Dwivedi et al., 2022). Similar explorations have of course been made about the engenderment of knowledge and attitudes when considering tobacco, alcohol, and drugs among others. Terms that follow here and more widely are; (1) knowledge regards information which is known or is the result of learning; (2) attitudes are predispositions, positive or negative, to certain objects or behaviors; (3) subjective norms are a person's belief about the likelihood that a particular behavior will be seen unfavorably by a certain group of people (Huang et al., 2021). It is argued from that perspective that these elements are likely interconnected in an environment where a lack of knowledge in general is evident – online safety and the internet. Further this is significant to consider in the context of attitudes and subjective norms as perceptions of the internet and the presentation of such are as various as those probing them (Teimouri et al., 2018).

Considering the vulnerable nature of young Internet users, university students are at significant risk of privacy breaches and cybercrime related to online banking and financial security. In the context of national campaigns and school interventions to improve online safety awareness, more comprehensive strategies are needed. Campaigns often address self-reporting by users to limit negative consequences, prevention measures for potential risks, and resistive strategies against undesirable information on websites. Such campaigns should address not only the recognition of possible risks but also the reservoir of 'defensive' information within students to prevent harm (Teimouri et al., 2018).

The framework illustrates key theories at the intersection of existing research on online behavior protection and appraises how such models can be applied to the current study focusing on online self-banking behavior of students. The centerpiece of the framework is formed with five model components. This first component is related to the understanding of the literature on online behavioral risks and acknowledgment of these risks about the usage of self-banking methods (Galdolage and Rasanjalee, 2022). Perceived risk refers to the belief of a particular risk and its seriousness. To avoid online risks, the individual should have risk perceptions of these risks. Thus, online risk awareness about online self-banking behavior may make students perceive themselves as vulnerable to these risks which, in turn, may increase the odds of taking precautions to deal with these risks. The second part defines the conceptual notions of online self-banking behavior protections (Grigorescu et al., 2023). The online self-banking behavior protection includes awareness-raising actions inappropriate and related risk channels of threats, preventive measures in terms

of installing multiple security tools, and taking precautions especially while conducting banking transactions.

METHODOLOGY

On 6th May 2020, the Australian Competition & Consumer Commission (ACCC) warned the public about an online phishing scam that targeted people with an expectation for a refund for overcharging. It comes to my attention that despite the prevalence of internet scams and high risks of being a victim of cybercrimes, there is a lack of comprehensive understanding regarding university students' risky online behaviors and their use of preventative measures. This position is evidently informed by the prominent literature on scam risks due to phishing emails and identity intelligence theft (Broadhurst et al., 2019).

Consequently, the massification of technology applications and the pervasive application of internet services are an important part of individual day-to-day activities. In the current Information Age, where information is seen as an important economic asset, the problem of data and information security is not to be taken lightly. Universities rely on information systems to carry out day-to-day operations such as recording students' results, recording financial records, and disseminating important information such as schedules and tuition (Ramlah Hussein et al., 2011).

College students who mostly involve in activities such as learning, online discussions, browsing and exchanging information through the internet arose the problem as these computer users are vulnerable to information security breaches. In addition, these computer users are identified as nonchalant in protecting information against information security breaches. This can take effect when these computer users consider the existence of computer security system installed in the application, such as antivirus, firewall, or instinct that data could still be safe. If the limitation is due to negligence on the part of the computer operator to manage information security, the various gap may occur due to an oversight could affect the nature of discipline and well-being in the workplace.

The research used a structured quantitative survey to measure the effectiveness of online safety awareness campaigns in reducing risky behaviors on the Internet. The hypothesis was confirmed that campaign acumen is important in reaching online safety-bothered students, and positively associated with online safety behavior, controlling for other correlates. University students were the focus; they are a high adopting, high utilizing, high distributing and high victimized group for using one of the most wide-spread Internet applications: the social networking sites. Due to these factors, the efficiency, success, and internet safety matters of awareness campaigns are highly questionable among them.

A structured quantitative survey was used to collect data. Six hypotheses were tested. The first three identify significant bivariate associations between the dependent variable, concerns about internet safety, and threat salience, campaign awareness, and counteraction motivation. University students were recruited using a convenience sample. Since the efficacy of these campaigns in a university environment is contested, they were also said to channel communications

towards those judged to be better resourced with cyber-knowledge, including employees; those in a position to teach safer practices, including IT services staff; and students residing in halls of residence. Posters were placed at 19 locations across the university and in six residential halls. 64.8% recalled seeing at least one of the three campaign features. Regarding the campaign content of posters, most student responses were uncertain on accurate awareness to the question on the number of reports that the campaign's fake email page received. Students were the sub-group with the greatest awareness of all features. Certainly, momentary awareness does have broader negative implications, austerity of results should remain paramount since the main objective is to present an initial empirical profile of the campaign and its likely impacts that can be utilized for more informed future strategies.

A survey was employed. Six universities were selected. 39 reporting units contained within the six universities were used as sampling frame. As a result, a response rate of 50% was achieved which represents a total of 195 academicians. Trend statistics as well as descriptive statistics were generated for each study objective. The findings suggest that it would be necessary in the long-run to focus more about managerial, security awareness and training elements, other than simply providing sophisticated technological devices. According to the results, academicians at the primary level tended to have a lower tendency to perform information security than at higher levels as compared to lecturers.

Data Collection and Analysis

Data was collected using an online student survey at a Malaysian university and focus groups by partnering with an on-campus IT department. The demographic characteristics of those surveyed include university students who were 221... All completed survey responses were analyzed using SPSS, except for an open-text response. Open-text data from survey answers was coded into themes before being analyzed. A subset of participating students was identified as being conducive to participation in focus groups. Of the individuals who took the survey and proactively agreed to participate in the study, a selection was made based on responses to demographic questions entered a random number generator. Focus group participation was also incentivized in the form of a raffle drawing for a gift card. To further represent those who had usable responses to the relevant open-text question, at least one student was selected from each of the three possible categories. Only one of these selected respondents eventually agreed to participate in the focus groups (Ramlah Hussein et al., 2011). Focus group results were transcribed. A single researcher then coded the data. Open-text responses made by focus group participants were also coded into relevant themes and are presented together with the findings of the larger student survey.

Before analysis, survey data was cleaned by excluding responses which indicated they do not currently attend the university associated with the research and by removing duplicate survey entries. Analysis was then conducted in a statistical software program; primarily, data was pulled into SPSS for all statistical analyses (Hill, 2017). Descriptive analyses were run on background information about survey respondents and on awareness and behavior variables

of interest. Finally, mean scores of scaled responses were compared between those who had seen campaign messaging and those who had not seen campaign messaging. Focus group data was transcribed and analyzed using a coding framework developed a priori. The most relevant and interesting themes which emerged from survey open-text responses are presented, and they are further decontextualized by incorporating relevant quotations from focus group participants. Throughout analysis, every attempt was made to ensure data integrity and transparency in the research process.

To address the research questions and test the hypotheses of a study, quantitative data has been acquired through a structured survey. In particular, the survey is used to assess the effectiveness of online safety awareness campaigns in altering students' online habits. Owing to the complexity and nuanced responses that can arise from these questions, some data is also captured through semi-structured interviews. Here, respondents can clarify their responses, provide additional context, or simply elaborate on their answers. Upon acquiring these survey and interview datasets, quantitative responses are analyzed through statistical tests. Ultimately, data is anonymized, cleaned, and formally analyzed through computer software. Qualitative responses are organized into themes based on pre-determined questions for respondents. All interview data is transcribed, coded, and analyzed within the boundaries of these themes. Importantly, the analysis process also includes a description of how data is moved from the stage of raw information to actionable and coherent findings (Makleff et al., 2021).

Concerning data collection, it is performed on a university campus. This is a setting where students are willing to undertake a survey at a time that best suits them. To achieve this, the survey administration is online, and its link is shared through various university group chats and emails. Additionally, ethical permission is obtained to undertake brief surveys in designated public areas of the campus. Here, students can take the survey from their own phone or computer. Moreover, semi-structured interviews are carried out with a pre-chosen set of 15 students. These students receive an email invitation and are asked to reply by confirming attendance. Notification and further details are also given regarding the subject material of the interview, the time commitment expected, and the format of the interview itself. Two day-long interview sessions are held, with a break in between for data cleaning and preliminary analysis. Each series of 15 interviews is performed by a pair of authors, rotating the interviewers to avoid the same interviewer-interviewee combinations each time. Interviews are audio recorded and later transcribed, so that nothing is missed due to bias or human error during the note-taking process. Each student is compensated with a small amount after the conclusion of the interview to match the time spent.

RESULT

Findings and Discussion section contains the results of data analyses in this same document. A qualitative + quantitative mixed method research was used. Data was collected from 35 university student participants. A qualitative in-depth personal interview was used to answer the first research question on

why students engage in risky behavior online. In addition, a survey was distributed to 1,039 university students. Significant model testing, using logistic regression was used to answer the second research question on the effectiveness of two university cyber safety awareness campaigns. Pairwise comparisons were made using McNemar's test. The results section also highlights the emergent themes and illuminates what the numbers reveal about student behavior while online.

The Cyber Security Password Awareness Campaign (CyberSAC) targeting undergraduate university students aimed to improve online safety while online. The situation is poignant: technology is evolving rapidly, whereas the general and university public may still lack basic safety skills (L. Innocenzi et al., 2018). Some students' e-behavior is deemed risky. Despite the gravity of online risks, many students take things lightly. Reports of hacks, identity theft, or malware intrusion are heard with detachment and face computer monitors displaying questionable web pages with an indifferent shrug. In previous studies, the amplification of impacts of digital crimes due to digitization is noted-however, these appeals were too boring and dry for students to relate to (Hill, 2017). As online security praxes see minimal adoption, students and staff members fall for even the most basic phishing scams; trainings quickly slaughtered by the pop-up window. That is the initiation of a deeper peek to analyze why students don't give a tweet about cyber security and what a forgotten folder in the recycle bin reveals about identity theft. Just like preschoolers don't and won't stop running everywhere (including in front of moving vehicles), it is vitally important to raise cyber security coolness in students (like some preschoolers are huge fans of running around in the garden – hence enticing the adoption of VPN outside campus. Professional terms are employed in moderation: unnecessary instructions on pesticides are not recited; the nature and challenges behind online security are illustrated without vaulting beyond interest).

A growing number of studies have highlighted the risks of phishing and other cybercrimes, especially online fraud, in various population subgroups. Young and apparently digitally savvy university students, however, have received less attention, even though they are particularly exposed to online threats. This study closes this gap by examining university students' scam susceptibility and risks of being in contact with phishing in the context of their everyday online academic and leisure activities.

The interaction of culture and scam susceptibility and personal IT competence and Internet safety more closely reflects a recent advance in understanding in these areas. Fieldwork was conducted in an Australian university within a narrow-defined time span. Participants were randomly selected on-campus, population-based sample of students in a direct observational period. Initial analytical modelling was followed by multivariate analysis of socio-demographic and behavioral data. This allowed us to track risks of being targeted by cybercrime and contributing factors for these risks. The data suggest that risks of being targeted by cybercrimes through text and email are strongly associated with academic engagement, affect females

disproportionately, and are markedly higher among students who have fallen for a fake scheme in the past. Findings suggest that frequenting webmail, downloading app and using the internet out of home could significantly increase risks. Conversely, having a high level of IT competence seems to provide protection against online threats. Since low personal IT competence is generally associated with vulnerable sectors, targeting these for prevention purposes should be further developed. Finally, attempts to increase feelings of safety on the Internet should be moderated in order that students are not complacent towards many potential cyber threats.

DISCUSSION

Theoretical implications and conclusions draw parallels to broader risks of harm associated with advertising and consumer culture, as well as those unique to an online context. Despite the complexity of this phenomenon, most individuals are still learning to become better consumers and producers of information on the internet in a rich media environment saturated with advertising. This extended social learning perspective is recommended as a completer and more adaptive theoretical framework for future research.

The campaign perceived there was a gap: young adults were the most prolific sharers of news online, but this was combined with the lowest engagement with news sources, limited acknowledgement of broader responsibilities about sharing, and the weakest digital literacy and online safety skills. This indicated a potentially dangerous, perhaps explosive, mix. In the present paper, it was suggested that as with greater power must come greater responsibility, it was similarly acknowledged that with greater capabilities platforms and consumers of the fast paced, navigable, widespread, and instantaneous flow of information must take on new skills and knowledge about the responsibilities and power vested in them. For this generation, internet access and usage are not new, but much about how big digital multinationals operate is still a black box. At the same time, there is also the rise of 'fake news', where even the 'news feed' was co-opted by interests and promoted narratives. The scope of the campaign was therefore broad, the paper wanted to hit upon issues that resonated with certain aspects of the campaign, and to develop an effort to cultivate a generation of savvier online sharers who approach sharing and lapping up of information with a more discerning and critical mind (L. Innocenzi et al., 2018). Social learning theory beautifully accounts for the passage from explicit teaching of new skills to role modelling best practices, verbal dissemination of new norms and practices, to the translation of such norms into day-to-day practices.

This paper attempts to test the short-run effects of a novel online safety awareness campaign on a group of university students using a specially designed app. An extensive body of experimental and quasi-experimental studies has attested to the alarming magnitude of harmful outcomes of risky online behavior. University students conform to one of the most vulnerable groups in this respect.

Awareness campaigns that aim to highlight specific risks and provide advice, guidelines, or training on how to adopt safer online habits are among the

most common tools used to reduce risky online behavior. Their effectiveness, however, has not been conclusively settled. On one hand, several studies confirm that properly designed online awareness media can indeed contribute to greater online security. On the other hand, experimental and quasi-experimental studies report that generally it is rather hard to ascertain that a given campaign can produce tangible effects in terms of healthier online behavior. This study contributes to the ongoing debate by providing evidence on the effectiveness of an app devised to reduce risky online behavior of university students (Teimouri et al., 2018).

The paper shows that this kind of digital campaigns may be effective in increasing online safety among university students through three avenues: a decrease in the time spent online, in visits to risky websites, and in sharing information about sensitive matters. Reduced online time and sharing online less information clearly bets well with the campaign's underlying aim. As far as the lower probability of visiting potentially harmful websites is concerned, it is quite interesting that such reduction takes place mostly because of the response of heavy users, while an increased probability of visiting risky sites is observed for younger individuals who use the Internet less intensively.

Implications for Practice

University students can be easily influenced by their online environments, resulting in risky online behavior. Thus, providing effective online safety awareness is essential. Considering the significant effect of the classroom-based format of online safety awareness campaigns and safety literacy, colleges may consider embedding online safety education into on-campus curricula. These findings present colleges with an opportunity to improve and enhance existing classroom-based formats of online safety awareness campaigns. To develop a more effective classroom-based format of an online safety awareness campaign, colleges need to adopt online safety campaigns employing a classroom-based teaching method. These online safety awareness campaigns should clearly define the effects of possible risks to help students easily identify them and prepare appropriate responses and solutions. Online safety campaigns should also transform complex and professional knowledge into fun and easy-to-understand animations and interactive quizzes. However, educators should pay attention to maintain interest and understanding at the same time.

Safety education providers can collaboratively work with colleges to develop online safety awareness campaigns that are tailored to student needs by continuously updating intervention content to match the most up-to-date and pressing trends, such as those observed during the COVID-19 pandemic. Results further suggest that incorporating online safety education into existing curricula can better reach students by promoting better understanding of the concepts and theories that underpin student learning and ultimately reduce risky behavior. Thus, collaborative efforts should be made by policymakers, safety education providers, and universities to address the lack of statutory requirements for including state educational entities in establishing measures for improving the safety of the educational environment, particularly the student's social environment, and to consider integrating online behavior safety modules into

undergraduate curricula. There is still a lack of legislative basis governing safety behavior in the field of online activities. To discourage and reduce negative online behavior, providing appropriate education, creating guidelines, and establishing a legal framework and administrative mechanisms to protect the victim must be considered. Online education safety campaigns should be launched on an ongoing basis. Due to the rapid development of the online environment, students lack skills in recognizing and responding to negative online behavior or finding relevant resources. To help these people face online challenges, additional resources and mentors should be provided.

The purpose of the research was to identify effective strategies for reducing risky online behavior among university students that can support the design of online safety awareness campaigns. A mixed-methods design collected and analyzed survey data on awareness levels of online risks and exposure to various types of risky online behaviors among undergraduate students. A focus group with participants then explored in more detail their understanding of online risks and their firsthand experiences with those risks. The results of the study suggest student-centric online safety awareness campaigns are likely to be more impactful at influencing student behavior. Raising online safety awareness by providing information on different online risks, particularly those related to student safety, could better prepare students to spot and avoid potential risks. The messages that can capture the attentions of students should be tailored to their interests. In collaboration with other departments, IT departments should be ready to provide support that goes beyond technical advice, such as sharing information on how to report phishing emails. If the aim is to develop safer online habits among students, the message should be continuously reinforced through regular safety education across all media and be mainstreamed in all student communication materials. With emphasis on providing training to university staff on how to spot online risks, those who work closely with students can deliver key safety messages not only quickly but also directly. In addition, support mechanisms should be established for first-time victims, such as running a cyber clinic, to help them recover effectively from different types of victimization.

CONCLUSIONS AND RECOMMENDATIONS

In the 21st century digital era, the internet has been fully incorporated into everyday life. The internet has incredibly empowered society in every aspect, facilitating greater collaboration, knowledge building, and information sharing. However, the internet is also a late modern invention, it promises certain risks in society that can lead to physical and emotional safety issues. Everyone is at risk of being exposed to these safety issues, directly or indirectly, actively or passively, willing or not. Risks from internet use are even more uncertain for students. Students are the agent of change and the future of society. When entering the university level of education, students are literate and vital in the digital era. On the one hand, as digital natives, they are expected to have the technological skills to avoid risks. On the other hand, they are faced with digital immigrants due to environmental pressures and demands, and parents, teachers,

and the surrounding environment have certain expectations in the use of technology and internet (Jang & Ko, 2023).

The main research questions that this study aims to address are as follows: What is the extent of online internet uses and online behavior awareness of university students? Can the implementation of online safety awareness campaigns contribute a decrease in risky online behavior among university students? The main objective of the study is examining the effectiveness of online safety awareness campaigns in reducing the risky online behavior of university students. The main hypothesis will be that an online safety campaign can decrease risky online behavior among university students. The purpose of this study is to assess online internet use uncertainty in a sample of university student and to explore how students' online behavior awareness behaviour predicts levels of risky online behavior with regards to the education of online safety strategies.

Research on the effectiveness of online safety awareness campaigns is limited. The present study aims to uncover the impacts of online safety awareness campaigns on the perceptions of online safety, as well as the effects of such campaigns on the reduction of risky online behavior. The study focuses on university students who are regarded as digital natives living in an expansive digital world and often show risky online behavior. To identify the mediating role of online safety perceptions, the Health Belief Model is adopted. Results show that online safety awareness campaigns directly reduce risky online behavior. It is found that beliefs in the seriousness and susceptibility of online safety threats, self-efficacy and effectiveness of protective behaviors significantly decrease risky online behavior, partially mediating the effects of campaign exposure.

Online safety awareness campaigns can play a significant role in reducing risky online behavior among university students. It is necessary to further investigate such impacts on internalizing the perceptions of online safety and to formulate an effective way of mediating them, which also has significant implications for campaign design and direction. While being regarded as digital natives, university students must still be addressed through single and web-based educational programs on online safety. Consequently, a considerable amount of online safety education for university students should aim to raise their awareness campaigns targeting risky online behavior (Teimouri et al., 2018). Since risky online behavior is a serious problem among university students, it is important for them to foster the improvement of educational strategies that implement online safety practices and decrease risky online behavior.

REFERENCES

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*. sciencedirect.com

Ayyoub, H. Y., AlAhmad, A. A., Al-Serhan, A., Al-Abdallat, M. F., Boshmaf, H., Abu-Taleb, Y. A., ... & Alshamaileh, Y. (2022). Awareness of electronic crimes related to E-learning among students at the University of Jordan. *Heliyon,* 8(10). cell.com

Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen Fan, Y. (2019). Phishing and Cybercrime Risks in a University Student Community. [PDF]

Chowdhury, E. K. (2024). Examining the benefits and drawbacks of social media usage on academic performance: a study among university students in Bangladesh. *Journal of Research in Innovative Teaching & Learning*. emerald.com

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., ... & Wamba, S. F. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International journal of information management*, 66, 102542. sciencedirect.com

Flayelle, M., Brevers, D., King, D. L., Maurage, P., Perales, J. C., & Billieux, J. (2023). A taxonomy of technology design features that promote potentially addictive online behaviours. *Nature Reviews Psychology*, 2(3), 136-150. researchgate.net

Foroutan, R. A., Sarokolaei, M. G., & Rezaeian, J. (2022). Online Customer Behavior: An Analysis of the Effects of Cognitive and Affective Trust. *Current Chinese Science*, 2(6), 434-449. researchgate.net

Galdolage, B. S., & Rasanjalee, R. S. (2022). Why do people move towards self-service technologies? Insights from banking sector in Sri Lanka. *Journal of Business and Technology*, 6(1). sljol.info

Grigorescu, A., Oprisan, O., Lincaru, C., & Pirciog, C. S. (2023). E-Banking convergence and the adopter's behavior changing across EU countries. *SAGE Open*, 13(4), 21582440231220455. sagepub.com

Hill, B. (2017). Parents perceptions of the internet and its effects on their children. [PDF]

Huang, H. L., Cheng, L. K., Sun, P. C., & Chou, S. J. (2021). The effects of perceived identity threat and realistic threat on the negative attitudes and usage intentions toward hotel service robots: the moderating effect of the robot's anthropomorphism. *International Journal of Social Robotics,* 13, 1599-1611. [HTML]

Jang, Y. & Ko, B. (2023). Online Safety for Children and Youth under the 4Cs Framework—A Focus on Digital Policies in Australia, Canada, and the UK. ncbi.nlm.nih.gov

Khaund, T., Kirdemir, B., Agarwal, N., Liu, H., & Morstatter, F. (2021). Social bots and their coordination during online campaigns: a survey. *IEEE Transactions on Computational Social Systems,* 9(2), 530-545. ieee.org

L. Innocenzi, R., Brown, K., Liggit, P., Tout, S., Tanner, A., Coutilish, T., & J Jenkins, R. (2018). Think Before You Click. Post. Type. Lessons learned from our University Cyber Security Awareness Campaign. [PDF]

Makleff, S., Garduño, J., Ivon Silva Márquez, V., Medina, S., Barindelli, F., & Marston, C. (2021). Collecting better data on sexuality, relationships and violence: empirical evidence from a school-based evaluation. osf.io

Mensah, G. B. (2023). Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems. *Preprint*. researchgate.net

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors,* 21(15), 5119. mdpi.com

Peterson, H. & Husu, L. (2023). Online panel work through a gender lens: implications of digital peer review meetings. *Science and Public Policy*. oup.com

Ramlah Hussein, *, Lambensa, F., & Baharuddin Anom, R. (2011). Information security behaviour : a descriptive analysis on a Malaysian public university. [PDF]

Schulte, P. A., Iavicoli, I., Fontana, L., Leka, S., Dollard, M. F., Salmen-Navarro, A., ... & Fischer, F. M. (2022). Occupational safety and health staging framework for decent work. *International journal of environmental research and public health*, 19(17), 10842. mdpi.com

Shabahang, R., Aruguete, M. S., & Shim, H. (2021). Online news addiction: Future anxiety, fear of missing out on news, and interpersonal trust contribute to

excessive online news consumption. *Online Journal of Communication and Media Technologies*, 11(2), e202105. ojcmt.net

Teimouri, M., Benrazavi, S. R., Griffiths, M. D., & Hassan, M. S. (2018). A model of online protection to reduce children's online risk exposure: *empirical evidence from Asia*. [PDF]

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 62(1), 82-97. researchgate.net