ISSN: 2182-2069 / E-ISSN: 2182-2077

The Impact of Internet Security Awareness among Undergraduates in Learning Management System

Dr. Segundo Juan Sanchez Tarrillo[1*], Dr. Rosa Guadalupe Neciosup Rosas[2], Dr. Evert José Fernández Vásquez[3], Dr. Eddy Miguel Aguirre Reyes[4], Dr. Henry Bernardo Garay Canales[5], Dr. Augusto Oswaldo Benavides Medina[6], Dr. Ruber Dennys Olaya Luna[7], and Dr. Jorge Luis Lopez Bulnes[8]

[1*]Research Professor, Escuela Pedagógica Publica Victor Andrés Belaunde – Jaén, Spain. jsanchez832@gmail.com, https://orcid.org/0000-0002-6763-760X

[2]Research Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. rneciosupr@unprg.edu.pe, https://orcid.org/0000-0003-1371-6051

[3]Research Professor, Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. efernandezv@unprg.edu.pe, https://orcid.org/0000-0002-0762-1382

[4]Research Professor, Universidad Nacional De Tumbes, Tumbes, Perú. eaguirrer@untumbes.edu.pe, https://orcid.org/0000-0003-1304-7601

[5]Research Professor, Universidad Nacional De Tumbes, Tumbes, Perú. hgarayc@untumbes.edu.pe, https://orcid.org/0000-0003-2323-1103

[6]Research Professor, Universidad Nacional De Tumbes, Tumbes, Perú. abenavidesm@untumbes.edu.pe, https://orcid.org/0000-0002-3017-7945

[7]Research Professor, Universidad Nacional De Tumbes, Tumbes, Perú. rolayal@untumbes.edu.pe, https://orcid.org/0000-0002-3115-8578

[8]Research Professor, Universidad Nacional Mayor De San Marcos, Lima, Perú. jlopezb@unmsm.edu.pe, https://orcid.org/0000-0002-9583-1143

Received: March 20, 2024; Revised: May 21, 2024; Accepted: June 24, 2024; Published: August 30, 2024

Abstract

The issue of Cybersecurity (CS) danger is a persistent and escalating burden that has garnered worldwide attention in recent years. This might be attributed to technological advances that have transformed the internet into a breeding ground for cybercriminals. The rising frequency of cybercrimes emphasizes the need for heightened CS Awareness (CSA) and education among individuals and institutions. This study investigates the level of CSA among undergraduates (UG). Surveys were sent to 250 UG from four chosen postsecondary institutions in Peru. The samples were selected using a basic random sampling procedure, and the gathered data was examined using percentages, frequencies, and statistical techniques such as regression and Analysis of Variance (ANOVA). They lacked awareness of effective measures to safeguard against cyber threats and assaults. A robust statistical correlation was found between the respondents' level of expertise in CS and their attitudes towards CSA. A substantial association was seen between their understanding of CS and their interest in CSA. The barriers that hinder CSA include a shortage of cyber talents, time

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 256-264. DOI: *10.58346/JISIS.2024.I3.015*

*Corresponding author: Research Professor, Escuela Pedagógica Publica Victor Andrés Belaunde – Jaén.

limitations, the absence of CS in non-computing programs, inadequate knowledge of essential computing regions, an absence of instructors with practical experience in CS, insufficient supportive facilities, and indifference. It is imperative to incorporate CS into educational programs to provide pupils with the necessary skills to navigate and safeguard against cyber threats, such as crime and espionage, in the current digital landscape, it is imperative to incorporate CS into educational programs to provide pupils with the necessary skills to navigate and safeguard against cyber threats, such as crime and espionage.

Keywords: Security, Learning Management System, Awareness, Undergraduates.

1 Introduction to Security in Learning Management System

Technological advancements and the widespread use of the internet and mobile devices have led to a rise in human behavior in the digital realm (Korte, 2020). According to the International Telecommunication Union (ITU), over half of the worldwide population, around 57.2%, or 5.2 billion individuals, are already employing the Internet. The growing population of online users has heightened the risks associated with Cyber Security (CS) and transformed the internet into a battleground for various cybercrimes (CC) (Al-Khater et al., 2020; Kaur & Ramkumar, 2022). Safeguarding data and content in the digital age has become increasingly crucial and complex. As organizations and companies transition their offerings to digital platforms or cloud-based systems, criminals are continuously escalating their methods to access, steal, and deceive individuals online illegally. The bad actions of cyber criminals have inflicted significant harm on people, organizations, enterprises, and institutions, presenting a grave threat to national security. Cybercriminals disguise themselves across numerous social media platforms (Jain et al., 2021). These have become a fertile breeding ground for intruders to breach privacy, manipulate and earn users' confidence, entice victims, and initiate fresh assaults (Li et al., 2021).

CC has become integral to daily existence as the boundaries between real life and the internet become increasingly blurred. Within the realm of education, the integration of technology into classrooms is becoming more prevalent as education systems progress (Tarrad et al., 2002). The primary reasons for integrating technology in education are likely the affordability of mobile devices and the internet and the undisputed and significant advantages of using Information and Communication Technology (ICT) (Al-Rahmi et al., 2020). This has resulted in classrooms being equipped with technological advances to enhance student learning more effectively and constructively. Relying on and using these ICT tools introduces novel and perilous CS vulnerabilities and menaces. As students increasingly use ICT technologies, they are becoming more susceptible to the dangers of disclosing sensitive personal information or accessing inappropriate content. Knowing CS is vital in minimizing and mitigating threats and assaults. It is crucial for all individuals who use the internet, particularly students in educational institutions, to comprehend the security hazards and dangers of internet usage.

Two catalysts have prompted the initiation of this investigation. First and foremost, students face many risks and dangers as internet users. Considering the level of CS Awareness (CSA) students possess upon graduating and entering the workforce is essential. Regarding the first point, while UG, like any average person on the Internet, are possible targets of cyber-attacks, their increased time spent online locates them at a higher risk. The danger escalates as most learners heavily depend on freely available items and even put their data and devices at risk by relying only on pirated antivirus programs for security. According to the CS Intelligence Score (CSIS), 93% of safety incidents are caused by human mistakes. These accidents often result in successful protection assaults when attackers manipulate individuals within businesses to get access to sensitive data (Fernando et al., 2024).

2 Background and Related Works

CS refers to the capacity to safeguard and shield the utilization of cyberspace from cyberattacks (Surendar et al., 2024). CS extends beyond the scope of conventional data protection by encompassing safeguarding not just data but other assets and individuals (Siddiqi et al., 2022). According to the ISO/IEC-27002 standard, data safety protects information regarding privacy, reliability, and accessibility (Fahrurozi et al., 2020). Within the ISO/IEC-27002 framework, data can manifest itself in many forms and presentations. The information can be reproduced physically by printing or writing on paper, saved in digital format, and transferred through traditional mail or electronic methods. Safeguarding data against potential risks, such as physical, human, and technical dangers, is necessary (Bonomi et al., 2020).

A CS risk refers to a situation or occurrence that can exploit weaknesses and cause adverse effects on the operations, resources, people, other institutions, or society as a whole. Kaspersky Support states that frequent cyber dangers to consumers include malware, which is harmful code that attempts to breach security (Rosa et al., 2024). This malware can be worms, trojans, viruses, malware, phishing attacks, spyware, risk wares, quips, rootkits, and spamming. 8500 cases were submitted to CS in Peru about the emergence of these risks.

The significance of CS knowledge has reached unprecedented levels. The frequency of private data breaches is rising, resulting in many daily identity theft cases (Burnes et al., 2020). Creating awareness among UG is the initial stage. By assessing the level of CS awareness, the effect of mitigating can be minimized by implementing suitable awareness programs. To effectively promote CS awareness in academic education, having a well-functioning and consistent framework for educational institutions is crucial (Dar et al., 2019; Jarl et al., 2021).

Based on the literature study, several studies have been conducted on the degree of CSA among UG (Payne et al., 2021). They have yet to focus on the university stage. The study was eager to investigate the level of knowledge regarding CS at a college in Peru. Peru is among the nations grappling with several CS-related challenges.

3 Materials and Methods

3.1. Sample Collection

The sample comprised 250 UG enrolled in regular online programs at a private institution in Peru. The UG used the method for determining the group's size, which ensures a 93% level of confidence and a 3% error tolerance. The data was acquired in October 2023 through an online Google Forms survey. Respondents were first advised that their survey involvement was private and voluntary. They were informed that the information they collected would be solely utilized for study purposes.

3.2. CSA Survey

A self-administered, structured survey to obtain participant data will result in more precise outcomes. A detailed survey tool was created to address the study problems and evaluate the hypotheses. A questionnaire, survey tool, or study tool is used to gather data in an investigation to fulfill the research goals. The research tool utilized in this research is a modified version of the CSA Survey. A survey was created to gather information on the demographics, computer proficiency and usage, and degree of awareness among students regarding CS. The questionnaire has 20 Likert scale items with three levels

to assess the degree of CSA among UG in northern Peru. Four additional items were included to gather data on the participant's demographic data (consisting of two inquiries) and the learner's proficiency and utilization of computing abilities (comprising of two things). These four items utilize the category attribute.

3.3. Verification of Research Tool

The content validity of topics on a Likert-type measure can be assessed by convening a panel of evaluators to analyze the items. The research developed the CSA Survey, and a senior academic professor from the University of Peru evaluated content validity. This professor possesses advanced knowledge and expertise in the specialized area of Educational Technologies and Multimedia. The tool was verified by three (3) instructors from the research site.

3.4. Reliability of Tool

A consistent pattern in successive measurements suggests a high level of dependability. Cronbach's Alpha (CA) is recognized as one of the most commonly used dependability measures. The reliability of the CSA Survey was assessed by administering it to 250 participants and analyzing the data using the Statistical Package for Social Sciences (SPSS). The CA score of inner consistency dependability for the CSA Survey was 0.742. The CA reliability factor often falls from 0 to 1. A higher coefficient value, closer to 1.0, indicates a more substantial internal consistency among the items (factors) in the ranking system.

4 Results and Discussions

4.1. Reliability Analysis

The assessment of internal consistency dependability for the 25-item is determined by computing CA. The CA for this assessment is 0.742. The calculated CA value demonstrates satisfactory internal coherence for the 25 elements, as shown in Table 1.

Table 1: CA reliability Analysis

CA score	Number of items
0.742	25

4.2 Demographic Data

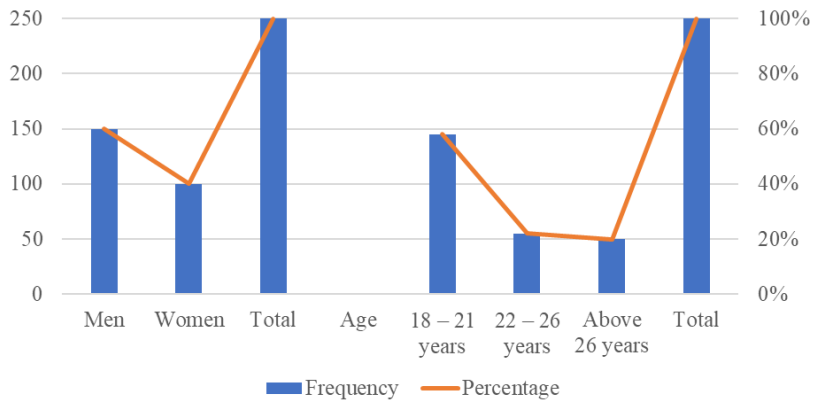

Figure 1: Demographic Detail and Age Analysis

Figure 1 illustrates the allocation of participants based on their gender and age. The data indicates that 60% of the participants were men, while 40% were women. This shows that almost all of the participants were men. The data reveals that 58% of the participants were 18 to 21, 22% were 22 to 26, and 20% were 26 years and above. This indicates that most participants fell between the age range of 18 to 21 years old.

4.3. Regression Evaluation

4.3.1. Prediction of CSA in UG

Table 2: Model Regression Analysis

Parameter	Value
R value	0.673
R-square value	0.327
Modified R square value	0.317
Standard error of the prediction	0.217

The regression results of the model is shown in Table 2. The R-value, the multifactorial correlation coefficient, measures the superficial similarity. In this case, the R-value is 0.673, indicating moderate similarity. The R^2, often known as the "R Square" columns, quantifies the proportion of the overall variance in the dependent factor that can be accounted for by the independent factors. The framework accurately fits the data obtained from the sampled UG in Peru, as indicated by the value of 0.327. This number provides an optimistic estimation of how well the framework fits the entire population. This is supported by the modified R^2, which has a value of 0.317. The modified R^2 is a measure that attempts to improve the accuracy of the R^2 number to reflect how well the framework fits the population. The independent factors account for 21.7% of the variation in the dependent factor.

The regression result details how much the model compensated for the variance, as shown in Table 3. The result for the total is the aggregate of the data for regression and excess. The framework explained a significant portion of the variance in the dependent factor due to the high value of the regression sum of squares, which was considerably more critical than the remainder of the squares value of 63.5. The framework effectively demonstrated its performance by the remaining sum of squares, 63.7. This implies that there is a statistically significant relationship between the factors.

Table 3: ANOVA Analysis

Parameter	Regression	Residue
Sum of squares	41.24	9.32
Degree of freedom	25	180
Mean square value	1.423	0.523
Variation	3.542	2.431

The T statistics facilitated the assessment of the relative significance of every factor in the framework. The relative relevance is established by the T values significantly less than -2 or more than +2. The UG's awareness and interest scores are over +2, with specific values of 3.132 and 3.523, respectively. All the autonomous factors are of significant value in determining the level of knowledge about CS amongst UG and their desire for CS courses. The independent factors effectively account for the variance in the dependent factor due to the very significant F statistic score of 0.001, which is below the threshold of 0.06. This indicates the presence of a significant association between the factors.

The coefficient of the predicted factor provides the numerical values used in the regression formula to predict the dependent factor based on the independent factor. These numbers represent the 93% confidence range for the parameters. The null hypotheses have been rejected. The data suggests that the extent to which students are knowledgeable about CS substantially impacts their attitudes toward CS and their enthusiasm for pursuing education in this field.

4.3.2. The Barriers to CS Awareness (CSA) among UG

The study utilized the Principal Axis Factor (PAF) with Promax rotations to analyze the obstacles hindering UG in CSA. Upon the initial examination of the R-matrix, a significant proportion of the variables exceeded the threshold of 0.25. The Kaiser-Mayer-Olkin (KMO) score was 0.79, higher than the required threshold of 0.5. Bartlett's Evaluation of Sphericity yielded a statistically significant result, suggesting that the information was appropriate for factor evaluation. The preliminary study yielded three components with Eigenvalues more critical than 1, accounting for 33.71%, 21.47%, and 9.42% of the variation. The initial element with an Eigenvalue greater than 1.0 and factors exhibiting factor loadings of 0.5 or higher can be selected as the threshold for permissible loadings. This criterion is significant in determining the lowest loading required for an item to be included.

Table 4: Total Variance Analysis

Factors	Eigen value	Variance (%)	Cumulative (%)
1	4.325	19	19
2	3.881	17.1	36.1
3	3.117	13.7	49.8
4	3.037	13.4	63.2
5	2.048	9	72.2
6	1.645	7.2	79.4
7	1.561	6.9	86.3
8	1.085	4.8	91.1
9	0.975	4.3	95.4
10	0.661	2.9	98.3
11	0.271	1.2	99.5
12	0.142	0.6	100

Table 4 shows the total variance analysis of the model. Adhering to the recommended guidelines for component retention, twelve components were selected for the final evaluation, consisting of three latent components. Factor 1 is characterized by five products: absence of qualified employees in CS, absence of appropriate facilities, limited time, a lack of attraction, and exclusion of CS in non-computing programs. Factor 2 is characterized by another five products: insufficient understanding of essential computing regions like computer design and operating system interiors, absence of instructors with hands-on expertise, lack of cyber training or complex programs, insufficient books on CS, and indifference. Factor 3 is characterized by two factors: cultural problems and network problems.

4.3.3. Discussion

The findings indicate that the participants need a more rudimentary understanding of CS. Many participants exhibited awareness of CS, although they needed more knowledge of effective measures to safeguard themselves from diverse cyber threats and attacks. The research considers their understanding of CS needs to be revised or improved. This aligns with the discovery that uncovered a need for

knowledge regarding CS among UG in Peru. The findings demonstrated a correlation between the extent of CSA among UG and their attitude toward CSA. Most respondents believed that CSA is crucial, given the escalating usage of the internet and the growing incidence of CC. There was a notable statistical correlation between the degree of awareness of UG and their curiosity about CS courses.

A significant number of respondents who were knowledgeable about CS dangers expressed their enthusiasm and readiness to participate actively in a CSA course. A strong level of student involvement enhances students' interest in CS. Increased participation of students in CS would improve their proficiency in cyber abilities. The findings indicate several barriers hinder CSA and education among UG in Peru. These barriers include a shortage of trained staff with CS expertise, insufficient resources for facilitating CSA, time limitations, the absence of CS content in non-computing programs, limited knowledge of essential computing regions, a lack of instructors with actual expertise in CS, a scarcity of cyber training or difficulties programs, and a shortage of publications on CS. Respondents in the study identified these variables as significant obstacles to their expertise and involvement in CS. If left unaddressed, these constraints can potentially restrict the extent of CS knowledge among UG in Peru.

5 Conclusion and Findings

Given the internet's widespread usage, which has become a refuge for cybercriminals, CS knowledge and education are now more essential than ever. Organizations should proactively implement steps to safeguard themselves against cyber risks and online fraudsters. Incorporating CS as a fundamental topic in all UG programs, particularly science-oriented universities, is imperative. This will facilitate knowledge acquisition regarding cyber dangers and the most effective methods of safeguarding oneself from cyber thieves, benefiting pupils, instructors, institutes, and companies in Peru. Promoting cultural or ethical principles is essential to discourage young individuals from participating in cybercriminal activities. The research is on how mobile devices impact the prevalence of CC in Peru and will create a mobile application to augment CSA in Peru in the future.

References

[1] Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. *IEEE Access, 8*, 137293-137311.

[2] Al-Rahmi, W. M., Alzahrani, A. I., Yahaya, N., Alalwan, N., & Kamin, Y. B. (2020). Digital communication: Information and communication technology (ICT) usage for education sustainability. *Sustainability, 12*(12), 5052. https://doi.org/10.3390/su12125052

[3] Bonomi, L., Huang, Y., & Ohno-Machado, L. (2020). Privacy challenges and research opportunities for genomic data sharing. *Nature Genetics*, *52*(7), 646-654.

[4] Burnes, D., DeLiema, M., & Langton, L. (2020). Risk and protective factors of identity theft victimization in the United States. *Preventive Medicine Reports, 17*, 101058. https://doi.org/10.1016/j.pmedr.2020.101058

[5] Dar, B. A., Ahmad, S., & Basharat, M. (2019). Use and Awareness of Digital Information Resources (DIRS) By Undergraduate Students: A Survey of Government Degree College for Women Anantnag, Jammu and Kashmir. *Indian Journal of Information Sources and Services*, *9*(1), 9–13.

[6] Fahrurozi, M., Tarigan, S. A., Tanjung, M. A., & Mutijarsa, K. (2020). The use of ISO/IEC 27005: 2018 for strengthening information security management (a case study at the Data and Information Center of the Ministry of Defence). *In IEEE 12th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 86-91.

[7] Fernando, E., Henry, B.G.C., Fernando, W.M.G., Carlos, M.A.S., Eddy, M.A.R., & César, A.F.T. (2024). Energy Efficient Business Management System for Improving QoS in Network Model. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 15*(1), 42-52.
[8] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems, 7*(5), 2157-2177.
[9] Jarl, M., Andersson, K., & Blossing, U. (2021). Organizational characteristics of successful and failing schools: A theoretical framework for explaining variation in student achievement. *School Effectiveness and School Improvement, 32*(3), 448-464.
[10] Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University-Computer and Information Sciences, 34*(8), 5766-5781.
[11] Korte, M. (2020). The digital revolution's impact on the human brain and behavior: where do we stand?. *Dialogues in Clinical Neuroscience, 22*(2), 101-111.
[12] Li, H., Yoo, S., & Kettinger, W. J. (2021). The roles of IT strategies and security investments in reducing organizational security breaches. *Journal of Management Information Systems, 38*(1), 222-245.
[13] Payne, B. K., Mayes, L., Paredes, T., Smith, E., Wu, H., & Xin, C. (2021). Applying high-impact practices in an interdisciplinary cybersecurity program. *Journal of Cybersecurity Education, Research and Practice, 2020*(2). https://doi.org/10.62915/2472-2707.1071
[14] Rosa, C., Wayky, A.L.N., Jesús, M.V., Carlos, M.A.S., Alcides, M.O., & César, A.F.T. (2024). Integrating Novel Machine Learning for Big Data Analytics and IoT Technology in Intelligent Database Management Systems. *Journal of Internet Services and Information Security, 14*(1), 206-218.
[15] Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences, 12*(12), 6042. https://doi.org/10.3390/app12126042
[16] Surendar, A., Saravanakumar, V., Sindhu, S., & Arvinth, N. (2024). A Bibliometric Study of Publication - Citations in a Range of Journal Articles. *Indian Journal of Information Sources and Services, 14*(2), 97–103. https://doi.org/10.51983/ijiss-2024.14.2.14
[17] Tarrad, K. M., Al-Hareeri, H., Alghazali, T., Ahmed, M., Al-Maeeni, M. K. A., Kalaf, G. A., & Mezaal, Y. S. (2022). Cybercrime challenges in Iraqi Academia: creating digital awareness for preventing cybercrimes. *International Journal of Cyber Criminology, 16*(2), 15-31.

Authors Biography

Dr. Segundo Juan Sanchez Tarrillo, Doctor in Education, Master in Educational Sciences with mention in Research and Teaching. Bachelor's degree in social sciences and philosophy. Professional with more than 15 years of experience in university teaching, developing curricular experiences of human formation and specialty.

Dr. Rosa Guadalupe Neciosup Rosas, Bachelor in Education. Bachelor in Sociology. Master in Educational Sciences, specializing in Higher Education and Educational Research. Teacher in Social Sciences, Sociologist by profession and researcher of folklore in Lambayeque, with completed doctoral studies in Educational Sciences and Sociology.

Dr. Evert José Fernández Vásquez, Bachelor's degree in Sociology. Bachelor in Education. Bachelor in Sociology. Master in Social Sciences with specialization in Social Policies. Ordinary teacher of the National University Pedro Ruiz Gallo.

Dr. Eddy Miguel Aguirre Reyes, Doctor in Education Administration, Master in Education with mention in Teaching and Educational Management and Master in Public Management, Public Accountant. Ordinary teacher of the National University of Tumbes.

Dr. Henry Bernardo Garay Canales, Research professor, doctor in education, master in public management, master in education, public accountant, undergraduate and graduate university professor, specialist in public management, thesis advisor and speaker in academic events.

Dr. Augusto Oswaldo Benavides Medina, Doctor in Administration. Master in Economics with mention in Business Management. Public Accountant. Main Professor at the National University of Tumbes.

Dr. Ruber Dennys Olaya Luna, Public Accountant. Master in Business Administration and Management. Master's Degree in Leadership from the Escuela de Alta Dirección en Administración-EADA, Spain. Doctorate in Administrative Sciences. Specialist in Public Management. University professor.

Dr. Jorge Luis Lopez Bulnes, PhD in qualitative research with emphasis on data analysis. PhD in Environment and Sustainable Development. Biologist with a Master's degree in education. Experience in university teaching and field research.