

# EXAMINING THE LINK BETWEEN INFORMATION SECURITY AWARENESS AND BEHAVIOR OF BASIC EDUCATION TEACHERS

Rexan E. Villaver & Nivea Louwah D. Sermona

Department of Technical and Technology Education  
University of Science and Technology of Southern Philippines  
rexanvillaver@gmail.com

**ABSTRACT:** *The Covid-19 pandemic has accelerated the adoption of digital technologies due to social distancing and lockdown measures. This shift is particularly evident in education, where there has been a significant move towards online communication and instruction. However, this rapid transition has also led to a surge in cyberattacks. The sudden switch to virtual classrooms without robust security measures in place resulted in an increase in phishing emails, compromised email accounts, and unauthorized access to databases and sensitive information. This study examined the level of information security awareness and information security behavior of public secondary school teachers, and the link between these two variables. The hypothesis that "there is no significant relationship between information security awareness and behavior of public secondary school teachers" was tested. This research study adopts a quantitative approach, focusing on the application of descriptive and correlational statistical analyses. A total of 59 randomly selected teachers from one public secondary school in Iligan City, Philippines compose the sample of this study. Teachers were asked to respond to information security awareness and behavior using adapted questionnaires. The results revealed that teachers generally have high levels of information security awareness (ISA) most especially on mobile device security measures. The information security behavior (ISB) of teachers, on the other hand, was collectively found to be at a medium level. The correlation between teachers' ISA and ISB was found to be moderately strong and positive, which means that the respondents with higher ISA are more likely to have higher ISB on the scale. Recommendations based on the results are presented in this paper.*

**Keywords:** basic education teachers, information security awareness, information security

## I. INTRODUCTION

The outbreak of the Covid-19 pandemic has necessitated a significant increase in the adoption of digital technologies, driven by social distancing measures and widespread lockdowns. Within the education domain, a profound transformation towards online modes of communication and instruction has been observed [1]. However, as a result of the rush to adopt e-learning, an increase in cyberattacks has been detected. Microsoft's Global Threat Activity Tracker identified over eight (8) million malware incidents, with education being the most affected industry from July to August 2020 alone [2]. Cybercriminals capitalized on opportunities to perpetrate school fraud, pilfer sensitive data, and execute ransomware schemes for extortion purposes. Since schools and universities were forced to switch to virtual classrooms quickly without adequately setting up a security strategy, there was a rise in phishing emails and compromised email accounts as well as unauthorized access to databases and sensitive information [3].

A White Paper Report of Cloudsek [4] showed that data collected in 2021 from various internet sources indicated that approximately 5% of identified threats were directed at educational institutions. This rise in cyber threats can be attributed to several factors, including the widespread adoption of remote learning during the COVID-19 pandemic, the digitization of educational materials, student data, and administrative processes, as well as the availability of online learning platforms.

Information security awareness pertains to an individual's understanding of potential security risks and the strategies available for thwarting these risks [5]. The viewpoint is that recognizing information security should form an essential component of the overall awareness possessed by members of the information society [6]. Conversely, Guo explained that information security-related behavior encompasses the actions of employees when utilizing organizational

information systems, including hardware, software, networks, and other elements that carry security consequences [7].

Much of the existing research on information security or cybersecurity in the education sector has primarily focused on higher education institutions [8, 9, 10, 11, 12] including the awareness and behavior of faculty members [13, 14]. There is a need for more studies specifically targeting basic education teachers, as they might have different experiences, and levels of technological literacy and face unique challenges in handling sensitive information.

Based on the foregoing literature, information security is a critical concern in today's digital landscape including the education sector, and understanding the relationship between awareness and behavior of teachers is vital for developing effective security interventions. Thus, this study examined the level of information security awareness and information security behavior of public secondary school teachers, and the link between these two variables. The hypothesis that "there is no significant relationship between information security awareness and behavior of public secondary school teachers" was tested.

## II. RESEARCH METHODOLOGY

This research study adopts a quantitative approach, focusing on the application of descriptive and correlational statistical analyses.

The questionnaire on information security awareness was adapted and modified from the study of Hammarstrand and Fu [15]. On the other hand, the Information Security Behavior questionnaire was adapted and modified from the study of Alohali, Clarke, Li, and Furnell measuring areas in password security, software security, email security, data management, and network management [16].

Both these instruments used a 5-point Likert Scale and were subjected to content validation by three information security experts and pilot testing with 30 teachers to measure their

respective internal consistency using Cronbach's alpha. The calculated Cronbach's alpha for the Information Security Awareness scale was 0.95, while 0.91 for Information Security indicating high internal consistency.

The participants for this study were randomly drawn from the complete list of teachers in one public secondary school in Iligan City, Philippines. Data from 59 respondents were used for the analysis after case-wise deletion of missing data. The respondents' age ranged from 31 to 62 years old with an average age of 44. Seventeen (17, 29%) of the respondents are males and 42 are females (71%).

Descriptive statistics were conducted to determine the level of information security awareness and information security behavior. Average score categories are obtained using an equal spacing scale scores partition. Specifically, we utilized the following scale scoring for ISA and ISB:

Score Range	ISA	ISB	
	Interpretation	Frequency	Level
1.00 – 1.79	Very Low	Never	
1.80 – 2.59	Low	Rarely	Low
2.60 – 3.39	Average	Sometimes	
3.40 – 4.19	High	Often	Medium
4.20 – 5.00	Very High	Always	High

To estimate the level of information security practice, respondents' frequency of performing information security activity (i.e., always, often, sometimes, rarely, and never) were gathered and were then codified into three levels (i.e., high, medium, and low). Responses for negatively-stated items were recorded for easy interpretation.

Spearman's rank correlation was used to measure the extent of the relationship between the two variables since it is robust to normality assumptions. In interpreting the strength of the correlation, the criteria of Best & Khan were used for this study [17], as follows:

Value	Description/Interpretation
0.00 – 0.19	Negligible
0.20 – 0.39	Low
0.40 – 0.59	Moderate
0.60 – 0.79	Substantial
0.80 – 1.00	High to very high

### III. RESULTS AND DISCUSSIONS

#### Teachers' Level of Information Security Awareness

The descriptive statistics result on the teachers' level of information security awareness is presented in Table 1.

**Table 1. Level of Information Security Awareness of Teachers**

Information Security Awareness on.....	Average	Description
Virus	4.10	High
Adware	3.10	Average
Spyware	3.25	Average
Phishing	3.78	High
Hacker	3.98	High
Firewall	3.73	High
Identity theft	4.03	High

Worm	3.34	Average
Trojan horse	3.37	Average
Anti-virus	4.22	Very High
Anti-spyware	4.15	High
Anti-spam	4.00	High
Software updates	4.20	Very High
Password security	4.27	Very High
Backups	4.24	Very High
Mobile device security measures	4.32	Very High
<b>Overall</b>	<b>3.88</b>	<b>High</b>

Results indicate that the overall level of information security awareness of teachers is high at an average of 3.88. In contrast, a study on the information security awareness of primary and secondary school teachers in Turkey was found to be moderate [18]. They found out that teachers who received information security awareness training and information technology teachers have higher awareness levels.

Moreover, the results further revealed that teachers' awareness of adware is lowest at an average of 3.10. Adware is the threat that delivers advertising content, often as pop-up windows that can slow or crash a computer can monitor or track the user's activities [19]. A study on the level of ICT competencies of basic education teachers from one public school in Tacloban City, Philippines showed that their knowledge of how to protect the computer from virus, spyware, adware, malware, hackers, and other threats are at the basic level only [20]. In contrary, a study conducted in a midsize southeastern university in Tennessee, USA showed that malware categories such as virus, Trojan, browser hijacker, adware, and ransomware were identifiable by faculty and staff [21].

#### Level of Teachers' Information Security Behavior

Data gathered shows that teachers' information security behavior is generally on a medium level (see Table 2).

**Table 2. Level of Information Security Behavior of Teachers**

Information Security Behavior	Average	Description
Password Security	3.65	Medium
Software Security	3.61	Medium
Email Security	3.74	Medium
Data Management	3.28	Low
Network Management	3.54	Medium
<b>Overall</b>	<b>3.56</b>	<b>Medium</b>

The National Bureau of Investigation (NBI) reported that teachers are visiting its cybercrime division to complain about their compromised bank accounts. The (NBI) has faced more complaints of cybercrime since the pandemic struck as the public relies on online banking transactions due to lockdowns during that period. The agency said that teachers have been victims of "phishing" and "vishing" scams intended to get a person's information through phone calls or messages for the scammer to get access to their bank accounts [22].

The results of this study also showed that security practice in data management which includes usage of external storage such as USBs and hard drives is found to be low. This is alarming to note, considering that effective data management is crucial for a growing organization, especially when it comes to tasks like managing staff, placing students, and handling recruitment, all of which are made easier with the use of computers [23]. In fact, it has been suggested that using good data management techniques will make future research in education and related fields better in quality [24].

**Relationship of Teachers’ Information Security Awareness and Behavior**

In this study, a Spearman rank correlation analysis was used to examine the relationship between the teachers’ information In a study that examined the information security and behavior of faculty and staff in a university, the results indicated that overall, faculty and staff had high to moderate levels of information security and behavior [14]. The same study revealed that teachers and staff who reported higher levels of security policy awareness demonstrated significantly more secure behaviors in 10 of the 18 items measured.

security awareness and behavior. The correlation coefficient (rho) was found to be significant at 0.50, indicating a moderately strong positive correlation ( $p < 0.00$ ,  $n = 59$ ). This means that the respondents with higher average ISA scores are more likely to have higher average ISB scores on the scale.

Variables Compared	Spearman’s Rho Correlation	P-Value	Remark
Average ISB Scores vs. Average ISA Scores	0.5040624	0.00004698	Significant at 0.05.

**IV. CONCLUSION**

Based on the results of the study, it is concluded that

- Teachers generally have high levels of information security awareness (ISA) most especially on mobile device security measures. However, teachers' awareness of adware, spyware, worm, and Trojan horse are only at the average level.
- The information security behavior (ISB) of teachers was collectively found to be at the medium level, but their security practice on data management which includes usage of external storage such as USBs and hard drives was found to be low.
- The correlation of ISA and ISB of teachers was found to be moderately strong and positive. This means that with higher levels of information security awareness, teachers are expected to have higher or better information security behavior.

**V. RECOMMENDATIONS**

Based on the conclusions, the following are hereby recommended:

- Providing security awareness training to teachers in primary education is recommended to reduce threats and safeguard the numerous information systems they have access to.
- It is advisable for the respective school administrators, or the Department of Education, in general, to establish policies relevant to information security as well as invest in teachers' training and information security infrastructure for the schools.
- Future research may be conducted employing qualitative approaches for an in-depth understanding of teachers’ information security awareness and behavior.

**VI. ACKNOWLEDGMENTS**

The authors wish to express their sincere gratitude to all those who contributed to the successful completion of this paper. Special mention to the respondents of this study, both during the pilot test and the actual survey, for generously sharing their insights and experiences, without whom this study would not have been possible.

**REFERENCES**

[1] Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, 55, 102171.

[2] Berkeley Extension (2020). Cybersecurity in Education: What Teachers, Parents and Students Should Know. Retrieved from <https://shorturl.ac/7b6no>

[3] Avey, C. (2021). Why Cybersecurity Should Be a Priority for The Education Sector. Retrieved from <https://rb.gy/attaj>

[4] Saxena, H. (2022). Cyber Threats Targeting the Global Education Sector on the Rise [White paper]. *CloudSEK Research Pte Singapore*. Retrieved from <https://rb.gy/i8lko>

[5] Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41

[6] Siponen, M. (2001). Five dimensions of information security awareness. *Computers & Society*, 31(2), 24-29.

[7] Sari, P. K., Handayani, P. W., Hidayanto, A. N., Yazid, S., & Aji, R. F. (2022). Information security behavior in health information systems: A review of research trends and antecedent factors. *Healthcare*, 10(12), 2531. MDPI AG. Retrieved from <http://dx.doi.org/10.3390/healthcare10122531>

[8] Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.

[9] Fouad, N.S. (2021) Securing higher education against cyberthreats: From an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6:2, 137-154, DOI: 10.1080/23738871.2021.1973526

[10] Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, 13(4), 192.

- [11] Sharma, A. (2021). Review on major cyber security issues in educational sector. *International Journal of Computer Sciences and Engineering* 9(12), 26-29
- [12] De Ramos, N.M., & Esponilla, F.D.E (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. *Int J Eval & Res Educ ISSN*, 2252(8822), 1199.
- [13] Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, 27(7-8), 241-253.
- [14] Yerby, J., & Floyd, K. (2018, August). Faculty and staff information security awareness and behaviors. *Journal of the Colloquium for Information Systems Security Education* 6(1), 23-23
- [15] Hammarstrand, J., & Fu, T. (2015). Information security awareness and behaviour-of trained and untrained home users in Sweden. Dissertation. Retrieved from <https://rb.gy/r113d>
- [16] Alohal, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and Predicting the Factors Affecting End-Users' Risk-Taking Behavior. *Information and Computer Security*, 26(3), 20. doi:<https://doi.org/10.1108/ICS-03-2018-0037>
- [17] Best, J. W & Khan, J. V. (2006). Research in Education (10th Ed.) New York: *Pearson Education Inc.*
- [18] Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology*, 13, 986561.
- [19] Yaseen, K.A.Y. (2022). Importance of Cyber Security in the Higher Education Sector 2022. *Asian Journal of Computer Science and Technology* 11(2), 20-24
- [20] Caluza, L.J.B., Verccio, R.L., Funcion, D.G.D., Quisumbing, L.A., Gotardo, M.A., Laurente, M.L.P., & Marmita, V. (2017). An assessment of ICT competencies of public school teachers: Basis for community extension program. *IOSR Journal of Humanities and Social Science*, 22(03), 01-13.
- [21] Quesinberry, M. (2016). An Analysis of Faculty and Staff's Identification of Malware Threats. *Electronic Theses and Dissertations*. Paper 3088. Retrieved from <https://dc.etsu.edu/etd/3088>
- [22] Owan, V. J., & Bassey, B. A. (2019). Data management practices in Educational Research. Owan, VJ & Bassey, BA (2019). Data management practices in educational research. In PN Ololube & GU Nwiyi (Eds), *Encyclopedia of institutional leadership, policy, and management: A handbook of research in honour of Professor Ozo-Mekuri Ndimele*, 1251-1265.
- [23] Odigwe, F. N., Bassey, B. A., & Owan, V. J. (2020). Data management practices and educational research effectiveness of university lecturers in South-South Nigeria. Odigwe, FN, Bassey, BA, & Owan, VJ (2020). Data management practices and educational research effectiveness of university lecturers in South-South Nigeria. *Journal of Educational and Social Research (JESR)*, 10(3), 24-34.