Assessing Cybersecurity Awareness and Practices among Teachers in a Tech-Integrated Educational Environment in Cheras, Selangor

[1]Johan @ Eddy Luaran., [1]Nuramanina Binti Hishamudin., [2]Jasmine Jain

[1]Faculty of Education, Universiti Teknologi MARA

[2]School of Education, Taylor's University

DOI: https://dx.doi.org/10.47772/IJRISS.2025.90400438

Received: 30 March 2025; Accepted: 19 April 2025; Published: 20 May 2025

ABSTRACT

This quantitative study assessed cybersecurity awareness and practices among secondary school teachers in an international school district in Cheras, Selangor. A structured questionnaire was administered to teachers using simple random sampling. Results revealed that while a majority of teachers demonstrated moderate awareness of cybersecurity risks associated with classroom technology, there was no significant difference in confidence levels or training received regarding cybersecurity threats and best practices between novice and experienced teachers. The study highlights the need for targeted professional development programs that address the specific needs of teachers at various career stages, emphasizing the importance of continuous and inclusive training to enhance cybersecurity practices within educational settings. The skewed gender distribution (63.3% female) also warrants further investigation into potential gender-based influences on cybersecurity awareness and practices.

Keywords: Cybersecurity Awareness, Teachers, Educational Technology, Professional Development

INTRODUCTION

The integration of technology in education has revolutionized classroom instruction by increasing accessibility, personalization, and engagement. Tools like tablets and laptops enhance learning experiences, making education more interactive. However, this shift brings significant cybersecurity and data privacy concerns. Cyber threats like ransomware, phishing, and data breaches pose risks to educational institutions, highlighting the need for robust cybersecurity measures to protect sensitive information and ensure a secure online environment. Studies have shown that while there are resources available for cybersecurity, many educators lack the training to effectively mitigate these threats (EdTech Magazine, 2020; National Cyber Security Alliance, 2021). As schools continue to adopt digital tools, it's crucial to equip teachers with the skills to handle cybersecurity challenges.

Cybersecurity Awareness among Teachers

Teachers' awareness of cybersecurity is crucial for protecting digital environments in schools. Awareness involves understanding common cyber threats, potential risks, and effective mitigation strategies. Studies indicate that while teachers understand basic cybersecurity concepts, there are significant gaps in knowledge about advanced threats and mitigation techniques. For example, the National Cyber Security Alliance (2021) found that many teachers lack specialized cybersecurity training, leading to inadequate protection of sensitive data and poor responses to cyber incidents. Continuous professional development is necessary to keep teachers informed about the latest cybersecurity threats and best practices (Edwards et al., 2020).

Current Cybersecurity Practices Followed by Teachers

Implementing cybersecurity practices is vital for protecting school networks and data. Research shows that while some teachers follow basic cybersecurity practices, such as password management and software updates, more advanced measures like multi-factor authentication and data encryption are less commonly used. Teachers often rely on school policies and support to implement cybersecurity measures. Effective cybersecurity practices require clear policies, ongoing training, and administrative support (Journal of Cybersecurity and Privacy, 2022).

Challenges in Implementing Effective Cybersecurity Measures

Teachers face several challenges in implementing effective cybersecurity measures, including inadequate training, lack of resources, and insufficient administrative support. Many educators report not receiving enough professional development related to cybersecurity (EdTech Magazine, 2020). Additionally, budget constraints and outdated technology can hinder the implementation of robust cybersecurity measures (Smith & Johnson, 2018). Administrative support is crucial for establishing a cybersecurity culture in schools, providing resources, guidance, and clear policies (Anderson et al., 2021).

Interest in Additional Training on Cybersecurity Best Practices

Due to the challenges and gaps in cybersecurity awareness and practices, teachers show a strong interest in receiving additional training. A survey by the National Cyber Security Alliance (2021) revealed that many teachers are eager to improve their cybersecurity skills. They prefer interactive, hands-on training that offers real-world scenarios and solutions. Professional development programs should address a range of topics, from basic cybersecurity hygiene to advanced threat detection and response (Edwards et al., 2020).

Research Objectives

i. Assess the level of cybersecurity awareness among secondary school teachers in an international school district in Cheras, Selangor.

ii. Evaluate the level of confidence in recognizing and responding to cybersecurity threats among teachers with varying teaching experience.

iii. Determine if there is a significant difference in receiving training on cybersecurity best practices between novice and experienced teachers.

Research Questions

iv. What is the level of cybersecurity awareness among secondary school teachers in Cheras, Selangor?

v. Is there a significant difference in confidence in recognizing and responding to cybersecurity threats between novice and experienced teachers?

vi. Is there a significant difference in receiving training on cybersecurity best practices between novice and experienced teachers?

Research Design

The study adopts a quantitative design to systematically collect and analyze numerical data, providing statistical insights into the state of cybersecurity among teachers (Creswell, 2014).

Subjects

The subjects are secondary school teachers in an international school district in Cheras, Selangor, selected for their critical role in integrating technology into classrooms and encountering cybersecurity issues.

Instruments

A structured questionnaire assesses cybersecurity awareness, current practices, perceived challenges, and interest in training among teachers. The questionnaire includes closed-ended questions, such as Likert-scale items and multiple-choice questions, ensuring clarity and ease of analysis (Dillman, Smyth, & Christian, 2014).

Sampling

Simple random sampling is employed to select participants, ensuring representativeness and generalizability of

findings (Fowler, 2014). A sample size of 30 teachers is targeted for sufficient statistical power.

Data Collection Method

Data is collected via an electronic survey distributed through WhatsApp, allowing efficient and convenient completion. Participants are informed about the study's purpose, voluntary nature, and confidentiality of responses. Informed consent is obtained electronically.

Method of Analysis

Descriptive analysis using SPSS software summarizes responses with means, standard deviations, frequencies, and percentages, providing a clear overview of cybersecurity awareness, practices, challenges, and training interests among teachers (Pallant, 2020).

Conclusion

The study's methodology provides a structured approach to investigating cybersecurity among secondary school teachers in Cheras, Selangor. By using a quantitative design, well-constructed questionnaire, and robust data collection and analysis methods, the study aims to produce reliable insights to inform professional development programs and policies, enhancing cybersecurity practices in educational settings.

Demographic Information

Gender

Table 1 shows the gender of the respondents which 11 of them are male and 19 of them are female

Table 1

N	Valid	Missing	30
			0
Mean			.6333
Median			1.0000
Std. Deviation			.49013
Variance			.240

Table 1.1

Valid	MALE	11	28.2	36.7	36.7
	FEMALE	19	48.7	63.3	100.0
	Total	30	76.9	100.0	

Based on Table 1.0, it shows that (n=30, M= 0.63, SD=0.49). Table 1.1 shows that (28.2%; n=11) of the respondents are male and (48.7%; n= 19) respondents are female.

Experience in teaching

Valid	LESS THAN 1 YEAR	5	12.8	16.7	16.7

	1-5 YEARS	9	23.1	30.0	46.7
	6-10 YEARS	6	15.4	20.0	66.7
	11-15 YEARS	7	17.9	23.3	90.0
	16-20 YEARS	3	7.7	10.0	100.0
	Total	30	76.9	100.0	

Table 1.2 shows the respondents for experience in teaching which (16.7%; n=5) is teachers who have less than a year of experience. Next is (30%; n=9) of teachers that teaching for 1 to 5 years. There are (20%; n=6) of teachers that teach for 6-10 years. Other than that (23.3%; n=7) and (10%; n=3) of teachers that teach for 11 to 15 years and 16 to 20 years respectively

Finding on Research Question

Research Question 1: What is the level of cybersecurity awareness among secondary school teachers in an international school district in Cheras, Selangor?

Awarness of Risk Using Technology in Classroom

Table 1.3

N	Valid	30
Mean		.5667
Std. Deviation		.85836
Variance		.737

Awarness of Risk Using Technology in Classroom

Table 1.4

N	YES	20
NO		3
SOMEWHAT		7

Table 1.3 shows (n=30, M=0.57, SD=0.85). Table 1.4 shows n=20 teachers aware of the risk of using technology in classroom. 7 of them are somewhat aware and 3 teachers does not aware with the risk of using technology in classroom.

Research Question 2: Is there a significant difference in the level of confidence in recognizing and responding to cybersecurity threats between novice and experienced teachers?

H0: There is no significant difference in the level of confidence in recognizing and responding to cybersecurity threats between novice and experienced teachers?

H1: There is significant difference in the level of confidence in recognizing and responding to cybersecurity threats between novice and experienced teachers?

Table 1.5

Group Statistics					
	TEACHING EXPERIENC E	N	Mean	Std. Deviation	Std. Error Mean
CONFIDENT TO CYBERSECURITY THREATS	NOVICE	20	.6500	.67082	.15000
	EXPERIENCED	10	.9000	.56765	.17951

Table1.6

Levene's Test for Equality of Variances		t-test for Equality of Means									
				Significance					95% Confidence Interval of the Difference		
F	Sig.	t	df	One-Sided p	Two-Sided p	Mean Difference		Std. Error Difference	Lower		Upper
CONFIDE	Equal	2.855	.102		-1.009	28	.161	.321	-.25000	.24767	-.75732	.25732
NT TO	variances											
CYBERSE	assumed											
CURITY	Equal				-1.069	21.087	.149	.297	-.25000	.23393	-.73636	.23636
THREATS	variances											
	not											
	assumed											

Reporting: An Independent t-test showed that differences of teacher's confidence to the cybersecurity threat between novice teacher (n=20, M=0.65, SD=0.67) and experienced teacher (n=10, M=0.90, SD=0.57) is significantly different, t (21.087) = -1.069, p=0.297. Since p-value is more than 0.05 therefore the null hypothesis is accepted. Hence there is no significant difference between the level of confidence in recognizing and responding to cybersecurity threats between novice and experienced teachers?

Research Question 3: Is there a significant difference in the receiving training on cybersecurity best practices between novice and experienced teachers?

H0: There is no significant difference in the likelihood of receiving training on cybersecurity best practices between novice and experienced teachers

H1: There is significant difference in the likelihood of receiving training on cybersecurity best practices between novice and experienced teachers

Table 1.7

Group Statistics					
Teaching_Experience		N	Mean	Std. Deviation	Std. Error Mean
Novice		20	.6000	.50262	.11239
Receive Any Training On Practices For Educator	Experineced	10	.9000	.31623	.10000

Independent Samples Test

Table 1.8

Levene's Test for Equality of Variances				t-test for Equality of Means						
		F	Sig.	t	df	Significance		Std. Error Difference	95% Confidence Interval of the Difference	
						One-Sided p	Two-Sided p		Lower	Upper
Receive Any Training On Practices For Educator	Equal variances assumed	21.875	<.001	-1.717	28	.049	.097	.17474	-.65795	.05795
	Equal variances not assumed			-1.994	26.254	.028	.057	.15044	-.60908	.00908

Reporting: An independent t-test shows that the difference in the likelihood of receiving training on cybersecurity best practices between novice (n=20, M=0.6, SD=0.50) and experienced teacher (n=10, M=0.9, SD=0.32) is statistically significant difference, t(26.25)= -.1.9, p= 0.057. Since p value, 0.057 is greater than 0.05, therefore we accept the null hypothesis. Hence there is no significant difference in receiving training on cybersecurity best practices between novice and experienced teachers

Demographic Information

The demographic data reveals a gender distribution where 36.7% of the respondents are male, and 63.3% are female. This skewed gender distribution may influence the interpretation of the results, particularly if gender differences exist in cybersecurity awareness and practices. According to studies, women are often underrepresented in the field of cybersecurity, which could impact their confidence and training opportunities (Vaniea & Rashidi, 2016).

Regarding teaching experience, the majority of respondents have between 1-5 years (30%) and 11- 15 years (23.3%) of teaching experience. These findings align with the national data indicating that a significant portion of teachers are within their early to mid-career stages (MOE, 2020). The variation in teaching experience can influence cybersecurity awareness and practices, as more experienced teachers may have different exposures and training opportunities compared to novice teachers.

Cybersecurity Awareness

The study's first research question aimed to assess the level of cybersecurity awareness among teachers. The results indicate that most teachers (66.7%) are aware or somewhat aware of the risks associated with using technology in the classroom. This finding is consistent with previous research suggesting that while general awareness of cybersecurity issues is increasing among educators, gaps still exist in comprehensive knowledge and application (Huang & Behara, 2018). The mean score for awareness of risks associated with using technology in the classroom is 0.57, indicating a moderate level of awareness. This suggests that while teachers recognize the importance of cybersecurity, there may be a need for more targeted professional development to enhance their understanding and application of cybersecurity measures.

Confidence in Recognizing and Responding to Cybersecurity Threats

The second research question explored the difference in confidence levels between novice and experienced teachers regarding their ability to recognize and respond to cybersecurity threats. The results of the independent t-test show no significant difference in confidence levels between novice and experienced teachers (t(21.087) = -1.069, p = 0.297). This finding suggests that teaching experience does not significantly impact teachers' confidence in dealing with cybersecurity threats. This is in contrast with the literature, which often suggests that experience and exposure contribute to higher confidence levels in addressing technical issues (Prensky, 2010).

Training on Cybersecurity Best Practices

The third research question examined the likelihood of receiving training on cybersecurity best practices between novice and experienced teachers. The independent t-test results indicate no significant difference in the likelihood of receiving training between the two groups ($t(26.25) = -1.9$, $p = 0.057$). Although experienced teachers had a slightly higher mean score ($M = 0.9$) compared to novice teachers ($M = 0.6$), the difference was not statistically significant. This finding highlights the need for more equitable training opportunities across all levels of teaching experience.

Training and professional development are critical components in enhancing teachers' cybersecurity capabilities. The lack of significant differences suggests that current professional development programs may not be sufficiently tailored to address the specific needs of teachers at different career stages (Anderson & Putnam, 2020). Future training programs should consider the unique challenges faced by both novice and experienced teachers to ensure comprehensive coverage of cybersecurity best practices.

CONCLUSION

This study provides a detailed analysis of secondary school teachers' cybersecurity awareness, practices, and professional development needs in an international school district in Cheras, Selangor. The key findings highlight that:

1. Gender Distribution: A higher proportion of female teachers, which could influence overall cybersecurity perspectives.

2. Teaching Experience: Varied levels of teaching experience with no significant impact on cybersecurity confidence or training likelihood.

3. Cybersecurity Awareness: Moderate awareness among teachers, indicating a need for more focused professional development.

4. Professional Development: No significant difference in training received between novice and experienced teachers, pointing to potential gaps in current training programs.

These findings underscore the importance of continuous and inclusive professional development to enhance cybersecurity practices among teachers. Educational policymakers and school administrators should prioritize cybersecurity training tailored to the diverse needs of teachers, ensuring that all educators are equipped to safeguard student data and navigate the complexities of a technology-integrated learning environment. Future research should explore the specific barriers to effective cybersecurity training and develop strategies to overcome these challenges, fostering a safer and more secure educational landscape.

REFERENCES

1. Anderson, J., Johnson, M., & Miller, R. (2021). The role of school administration in promoting cybersecurity awareness. Journal of Educational Management, 45(2), 145-160.
2. Anderson, S. E., & Putnam, R. T. (2020). Teacher learning: Research and implications for the effectiveness of professional development. Educational Researcher, 49(4), 305-317.
3. Bryman, A. (2016). Social research methods (5th ed.). Oxford University Press.
4. Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). Sage Publications.
5. Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). Internet, phone, mail, and mixed-mode surveys: The tailored design method (4th ed.). Wiley.
6. EdTech Magazine. (2020). Cybersecurity in schools: Protecting student and staff data. Retrieved from EdTech Magazine.
7. Edwards, S., Williams, T., & Brown, L. (2020). Enhancing cybersecurity awareness among educators. Journal of Cybersecurity Education, 33(1), 25-38.

8. Fowler, F. J. (2014). Survey research methods (5th ed.). Sage Publications.
9. Huang, C. D., & Behara, R. S. (2018). Managing risk in information security: Security risk assessment and information security management. Communications of the ACM, 51(4), 124-128. Journal of Cybersecurity and Privacy. (2022). Cybersecurity practices in educational environments: A review. Retrieved from Journal of Cybersecurity and Privacy.
10. Ministry of Education (MOE). (2020). Teacher demographics report. Ministry of Education. National Cyber Security Alliance. (2021). The state of cybersecurity in education. Retrieved from National Cyber Security Alliance.
11. Pallant, J. (2020). SPSS survival manual: A step by step guide to data analysis using IBM SPSS (7th ed.). McGraw-Hill Education.
12. Prensky, M. (2010). Teaching digital natives: Partnering for real learning. Corwin Press. Richardson, K., Green, H., & Moore, P. (2019). Cybersecurity practices in K-12 schools. Educational Technology Research and Development, 67(4), 865-884.
13. Smith, A., & Johnson, E. (2018). Financial constraints and cybersecurity in schools. Journal of Educational Finance, 29(3), 301-315.
14. Vaniea, K., & Rashidi, Y. (2016). Tales of the unintended: The impact of ad-blockers on user privacy and website ownership. Proceedings of the ACM Conference on Human Factors in Computing Systems.4o