

CYBERSECURITY AWARENESS AMONG PRIMARY AND SECONDARY SCHOOL TEACHERS IN FUJIAN PROVINCE, CHINA: PREDICTORS AND ENHANCEMENT RECOMMENDATIONS

Huang Zhan^{1*} and Songpon Nakharacruangsak²

Master of Science Program in Information Technology,
Faculty of Digital Technology and Innovation, Southeast Bangkok University^{1,2}
Author email: 2199897066@qq.com¹, Songpon@southeast.ac.th²

Received: April	9, 2026
Revised: May	25, 2026
Accepted: June	15, 2026

Abstract

Against the backdrop of limited empirical research on teachers' cybersecurity awareness, particularly concerning the role of training frequency, this study aims to: 1) assess the current level of cybersecurity awareness among primary and secondary school teachers in Fujian Province, China; 2) identify its key predictors; and 3) propose targeted recommendations for improvement.

A quantitative questionnaire survey was employed, yielding 321 valid responses, and the data were analyzed using statistical software. Results indicate that respondents had a moderately above-average overall cybersecurity awareness. Gender, age, school location, and training frequency significantly predicted awareness levels, whereas educational background and digital tool usage frequency showed no significant effects. Training frequency exhibited a significant diminishing marginal effect, with 1–2 annual sessions delivering the most cost-effective improvement. This research provides empirical support for developing standardized cybersecurity training for teachers, and its key contribution lies in quantifying the optimal training frequency and offering actionable policy implications.

Keywords: Cybersecurity Awareness, Teachers, Predictors, Cybersecurity Training, Fujian Province

Introduction

With the rapid digitalization of education, primary and secondary schools face increasing cybersecurity risks. Cyberattacks against educational institutions are rising worldwide [1]. In 2023, global ransomware attacks increased by 84%, and education services became one of the top 10 targeted industries because schools store large amounts of sensitive personal data [1,2,3]. Therefore, cybersecurity capacity is essential for maintaining educational stability and protecting privacy [4].

Teachers are the first line of campus cybersecurity defense and important guides for students' digital literacy [5]. However, studies show that teachers in digital educational environments still face cybersecurity and digital risk challenges, including insufficient awareness, protection skills, and emergency response preparation [6,7]. Although countries such as the United States have included cybersecurity training in teacher continuing education [8], empirical research in China remains limited, especially on training frequency and regional evidence from Fujian Province.

Fujian Province, a pioneer in China's Digital China initiative, reached a 98.7% digital penetration rate in primary and secondary schools by 2024. The wide use of online teaching platforms, student information systems, and smart campus devices has increased cybersecurity exposure. Low teacher awareness may lead to ransomware risks, student data breaches, and weak guidance for students' digital safety. To address these gaps, this research investigates teachers' cybersecurity awareness in Fujian Province, identifies key predictors, and proposes evidence-based enhancement recommendations. Its findings provide empirical support for improving teacher cybersecurity training in China.

Research Objectives

1. To assess the current level of cybersecurity awareness among primary and secondary school teachers in Fujian Province, China, and systematically quantify their performance across the three core dimensions of cybersecurity cognition, protection skills, and emergency response capability.
2. To identify the key predictors of teachers' cybersecurity awareness, and empirically test the effects of demographic characteristics, technical experience, training experience, and school location on teachers' overall awareness level and each dimensional performance.
3. To propose targeted enhancement recommendations for improving primary and secondary school teachers' cybersecurity awareness based on empirical findings and teacher cybersecurity training practices [8].

Research Methodology

A quantitative empirical research design was adopted for this study, combining descriptive and correlational methods alongside literature research. This approach allowed for a systematic investigation of cybersecurity awareness among primary and secondary school teachers in Fujian Province and its predictors.

1. Research Subjects and Sampling

The subjects were primary and secondary school teachers in Fujian Province, China. From September to November 2025, stratified random sampling was conducted in urban and rural public and private schools in Fuzhou, Xiamen, Putian, and Nanping. Schools were stratified by location and type, and teachers were randomly invited.

A total of 362 questionnaires were distributed, 353 were returned, and 321 valid responses were retained after excluding incomplete, repeated, or abnormal responses. The effective recovery rate was 88.67%.

2. Research Instrument

A self-developed cybersecurity awareness questionnaire was revised and localized based on ENISA cybersecurity awareness materials [9] and the HAIS-Q [10]. It included six sections: demographic information, cybersecurity cognition, prevention skills, response capability, training and educational experience, and self-assessment and needs. The three core dimensions each contained 10 items measured by a 5-point Likert scale.

Higher scores indicated stronger cybersecurity cognition, more standardized protective behaviors, and better response capability. A pre-test with 30 teachers was conducted before the formal survey. The overall Cronbach's Alpha was 0.92, and the KMO value was 0.927, indicating good reliability and validity.

3. Variable Definition and Measurement

Independent variables included gender, age, education level, school location, digital tool use frequency, and cybersecurity training frequency. For analysis, gender was coded as male = 1 and female = 2, school location as urban = 1 and rural = 2, while age and education level were coded by category. Digital tool use frequency and cybersecurity training frequency were treated as ordered variables.

The dependent variable was teachers' overall cybersecurity awareness, calculated as the total score of cybersecurity cognition, prevention skills, and response capability [11]. Each dimension contained 10 items, with scores ranging from 10 to 50; the total score ranged from 30 to 150, with higher scores indicating stronger overall cybersecurity awareness.

The conceptual framework of variable relationships is illustrated in Figure 1.

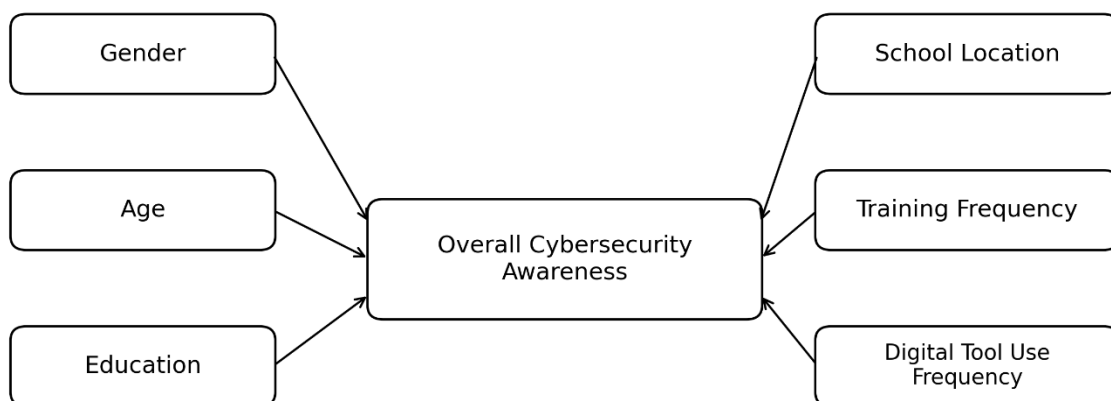


Figure 1. Conceptual Framework of Teachers' Cybersecurity Awareness Predictors.

4. Data Collection and Analysis

Questionnaires were collected online and offline. Participation was voluntary and anonymous, and academic ethics were followed.

Statistical software was used for analysis. Before inferential tests, normality, independence, and multicollinearity were examined. The methods included descriptive statistics, reliability and validity analysis, independent samples t-test, one-way ANOVA, Pearson correlation analysis, and multiple linear regression analysis.

Research Results

Statistical analysis was conducted based on 321 valid questionnaires from primary and secondary school teachers in Fujian Province, with an effective response rate of 88.67%. In line with the three research objectives, this section presents the preliminary analysis, the current level of teachers' cybersecurity awareness, the key predictors, and the empirical basis for enhancement recommendations.

5.1 Preliminary Analysis of the Sample and Research Instrument

Before addressing the research objectives, sample characteristics and scale quality were examined. As shown in Table 1, the valid respondents covered different genders, education levels, school locations, and cybersecurity training experiences, indicating acceptable sample representativeness.

Table 1 Demographic Characteristics of the Samples.

Variable	Frequency (n)	Percentage (%)
Gender		
Male	166	51.7
Female	155	48.3
Education Level		
Bachelor's degree or above	219	68.2
Below bachelor's degree	102	31.8
School Location		
Urban	191	59.5
Rural	130	40.5
Cybersecurity Training Experience		
Participated	144	44.9
Not participated	177	55.1
Total	321	100

The reliability and validity results are shown in Table 2. The overall Cronbach's Alpha was 0.92, and all dimensions exceeded the 0.70 threshold. The KMO value was 0.937, and Bartlett's test was significant at $p < 0.001$, suggesting that the questionnaire had good reliability and construct validity.

Table 2 Reliability and Validity Test Results.

Test Index	Criterion	Value	Result
Cronbach's α (Overall)	> 0.70 (Good)	0.92	Excellent
Cronbach's α (Awareness)	> 0.70 (Good)	0.913	Excellent
Cronbach's α (Prevention)	> 0.70 (Good)	0.923	Excellent
Cronbach's α (Emergency Response Capability)	> 0.70 (Good)	0.917	Excellent
KMO	> 0.60 (Suitable)	0.937	Very suitable
Bartlett's Test	$p < 0.001$	0	Significant

5.2 Findings Related to Research Objective 1: Current Level of Teachers' Cybersecurity Awareness

To address the first research objective, teachers' cybersecurity awareness was measured across three dimensions: cybersecurity cognition, protection skills, and emergency response capability. As shown in Table 3, the overall mean score was 112.76, indicating a slightly above-average level of cybersecurity awareness. Among the three dimensions, prevention skills scored the highest, while emergency response capability was relatively lower, suggesting that further improvement is needed in practical response skills.

Table 3 Overall Level of Teachers' Cybersecurity Awareness.

Dimension	Mean (M)	Standard Deviation (SD)	Evaluation
Cybersecurity Awareness	37.62	8.208	Slightly above average
Prevention Skills	37.7	8.544	Slightly above average
Emergency Response Capability	37.44	8.354	Slightly above average
Overall Total Score	112.76	24.562	Slightly above average

5.3 Findings Related to Research Objective 2: Key Predictors of Teachers' Cybersecurity Awareness

To address the second research objective, difference analysis, correlation analysis, and multiple regression analysis were conducted. As shown in Table 4, cybersecurity awareness differed significantly by gender, age, school location, and cybersecurity training experience, while education level showed no significant difference.

Table 4 Differences in Cybersecurity Awareness by Demographic Characteristics.

Variable	Group	n	Mean (M)	Standard Deviation (SD)	t/F	p	Significance
Gender	Male	166	117.39	23.12	4.831	<0.001	***
	Female	155	107.79	25.21			
Education Level	Bachelor's degree or above	219	113.25	24.87	0.741	0.478	ns
	Below bachelor's degree	102	111.72	24.03			
School Location	Urban	191	117.51	23.65	5.498	<0.001	***
	Rural	130	105.77	24.78			
Cybersecurity Training Experience	Participated	144	124.34	21.56	9.964	<0.001	***
	Not participated	177	103.28	23.89			
Age Group	≤25 years old	89	121.67	22.34	7.878	<0.001	***
	26–40 years old	156	113.42	24.15			
	41–55 years old	67	105.89	25.62			
	≥56 years old	9	102.11	26.78			

Note: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; ns = not significant

Pearson correlation analysis was conducted to examine the relationships among overall cybersecurity awareness, its three dimensions, training frequency, and teaching seniority. As shown in Table 5, overall cybersecurity awareness was positively correlated with cybersecurity cognition, protection skills, emergency response capability, and training frequency.

Table 5 Pearson Correlation Matrix of Variables.

Variable	1	2	3	4	5	6
1. Overall Cybersecurity Awareness	1					
2. Cybersecurity Cognition	0.892***	1				
3. Protection Skills	0.915***	0.786***	1			
4. Emergency Response Capability	0.873***	0.721***	0.794***	1		
5. Training Frequency	0.517***	0.380***	0.335***	0.405***	1	
6. Teaching Seniority	-0.146**	-0.152*	-0.174**	0.009ns	-	1

*Note. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; ns = not significant.

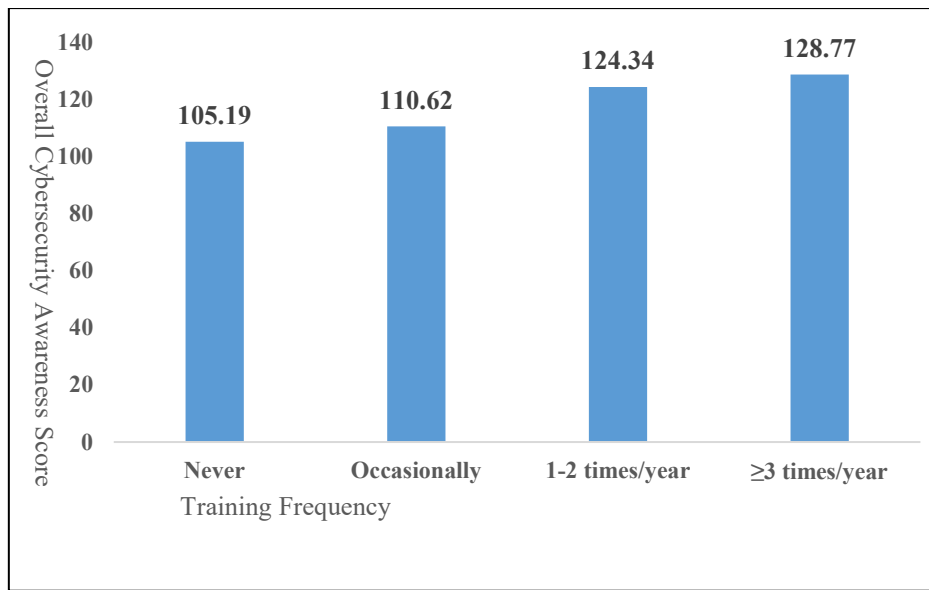


Figure 2 Overall Cybersecurity Awareness Scores by Training Frequency.

Figure 2 further illustrates the trend of overall cybersecurity awareness scores across different training frequencies.

As shown in Figure 2, awareness scores increased as training frequency increased, with a notable improvement among teachers receiving training 1–2 times per year.

To further identify the key predictors of teachers' cybersecurity awareness, multiple linear regression analysis was conducted. The results are shown in Table 6.

Table 6 Multiple Regression Analysis of Overall Cybersecurity Awareness.

Variable	Unstandardized β	Standardized β	t	p	VIF
(Constant)	125.059	-	23.232	<0.001***	-
Gender	-5.771	-0.159	-3.462	0.001***	1.056
Age	-3.064	-0.163	-3.594	<0.001***	3.077
Education Level	1.128	0.042	0.929	0.353ns	1.042
School Location	-7.358	-0.2	-4.292	<0.001***	1.073
Training Frequency	7.075	0.423	8.926	<0.001***	6.108
Frequency of Digital Tool Use	-0.527	-0.03	-0.668	0.504ns	1.029
Model Fit	$R^2 = 0.363$, Adjusted $R^2 = 0.350$, $F = 29.761$, $p < 0.001$ ***				

*Note. * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$; ns = not significant.

As shown in Table 6, the regression model was significant and explained 35.0% of the variance in teachers' cybersecurity awareness. Training frequency was the strongest predictor, followed by school location, age, and gender, while education level and digital tool use frequency were not significant predictors.

Table 7 Verification Results of Research Hypotheses.

Hypothesis Number	Hypothesis Content	Verification Result
H1	Teachers' technical experience is significantly positively correlated with their cybersecurity awareness	Not supported
H2	Teachers who have received cybersecurity training have significantly higher overall cybersecurity awareness than those who have not.	Strongly supported
H3	Teachers' educational background has a significant impact on their cybersecurity awareness	Not supported
H4	School location has a significant impact on teachers' overall cybersecurity awareness.	Supported
H5	Gender has a significant impact on teachers' overall cybersecurity awareness.	Supported

5.4 Findings Related to Research Objective 3: Empirical Basis for Enhancement Recommendations

To address the third research objective, recommendations were developed based on the empirical findings. Since training frequency was the strongest predictor, schools should establish a standardized annual cybersecurity training system, with 1–2 systematic sessions per year as a cost-effective baseline. As school location had a significant effect, more training resources should be allocated to rural schools. In addition, the relatively lower score of emergency response capability indicates the need for more scenario-based training, such as phishing email identification, ransomware response, student data leakage reporting, and emergency handling drills.

Overall, the results directly respond to the three research objectives: Table 3 presents the current level of teachers' cybersecurity awareness; Tables 4–7 identify the key predictors and verify the hypotheses; and the empirical findings provide evidence-based support for the proposed enhancement recommendations.

Conclusion and Discussion

1. Interpretation of Core Findings

The results show that cybersecurity training is the strongest predictor of teachers' cybersecurity awareness, highlighting the need for targeted training [8] and systematic teacher digital literacy development [12].

The findings align with PMT [13], as cybersecurity training may strengthen threat perception, response efficacy, and self-efficacy. The effect of school location is also consistent with TAM [14], since urban schools usually have better infrastructure and access to cybersecurity tools. Meanwhile, the non-significant effects of digital tool use and educational background suggest that general technology use and formal education are insufficient without targeted training, consistent with human factors cybersecurity research [15].

2. Theoretical Implications

This research supports the use of PMT [13], TAM [14], TPB [16], and SCT [17] to explain K-12 teachers' cybersecurity awareness. Systematic training can strengthen threat perception, protective motivation, perceived usefulness, and behavioral confidence. The differences by gender, age, and school location are consistent with prior findings [18].

Unlike previous studies [8,18,19], educational background and digital tool use frequency were not significant predictors. This suggests that general education and daily digital use do not necessarily improve cybersecurity awareness without targeted training. The findings clarify the boundary between technology use and cybersecurity awareness, and highlight the value of optimizing training frequency.

3. Practical Implications

The findings indicate that teacher cybersecurity awareness should be improved through systematic and targeted training. Since one-off cybersecurity awareness campaigns often fail to produce long-term behavioral change [20], education authorities should establish an annual training system.

Training resources should prioritize rural schools to narrow the urban-rural gap and strengthen rural teachers' digital literacy support [21]. Schools should also integrate 1–2 systematic cybersecurity training sessions per year into continuing education and strengthen teachers' role in building a collaborative protection system among teachers, students, schools, and families.

4. Limitations and Future Research

This research is limited by its regional sample from Fujian Province and its use of only quantitative methods. Future studies should expand the sample scope, adopt mixed methods, and use longitudinal designs to examine the long-term effects of different cybersecurity training modes.

Recommendation

1. schools should establish a standardized annual cybersecurity training system. Based on the findings, 1–2 systematic training sessions per year may serve as a cost-effective baseline. The training content should cover phishing identification, password management, data backup, and emergency reporting.
2. more cybersecurity training resources should be allocated to rural schools. Education authorities may provide shared online courses, regional training programs, urban-rural paired assistance, and remote technical support to reduce the urban-rural gap in teachers' cybersecurity literacy.
3. scenario-based training should be strengthened, especially in emergency response. Schools may organize practical drills on phishing email disposal, ransomware response, student data leakage reporting, and infected-device isolation to improve teachers' practical response capability.
4. differentiated training programs should be provided for teachers of different age groups and technical backgrounds. For older teachers, training should focus on basic risk identification and step-by-step emergency procedures. For younger teachers, training may emphasize advanced threat cases, privacy protection, and student guidance in digital environments.
5. teachers' cybersecurity literacy should be integrated into the overall campus cybersecurity education system. Schools may build a collaborative mechanism involving teacher training, student cybersecurity classes, parent-school communication, regular risk reminders, and campus cybersecurity culture construction to form a full-coverage protection system.

References

- [1] Flashpoint, *2024 Global Threat Intelligence Report*. New York, NY, USA: Flashpoint, 2024. [Online]. Available: <https://flashpoint.io/resources/report/2024-global-threat-intelligence-report/>
- [2] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2024*. Athens, Greece: ENISA, Sep. 2024, doi: 10.2824/0710888.
- [3] K. Qi, "A research on the application of virtual network technology in computer network security," *Journal of Electronic Research and Application*, vol. 6, no. 4, pp. 1–6, 2022, doi: 10.26689/JERA.V6I4.4153.
- [4] Z. Wang and T. Cheng, "Practical strategies and guarantee mechanisms for cybersecurity literacy education for primary and secondary school students in the United States," *Journal of Teacher Education*, vol. 10, no. 1, pp. 100–108, Jan. 2023. DOI: 10.13718/j.cnki.jsjy.2023.01.012
- [5] H. F. Sapanca and S. Kanbul, "Risk management in digitalized educational environments: Teachers' information security awareness levels," *Frontiers in Psychology*, vol. 13, Art. no. 986561, Aug. 2022. DOI: 10.3389/fpsyg.2022.986561
- [6] W. Chen, Y. He, X. Tian, and W. He, "Exploring cybersecurity education at the K-12 level," in *Proc. SITE Interactive Conf.*, E. Langran and D. Rutledge, Eds., Charlottesville, VA, USA: Association for the Advancement of Computing in Education, 2021, pp. 108–114.

-
- [7] Q. Zhao and L. Dai, "Digital risks for teachers in the digital age and the way to avoid them," *Journal of Teacher Education*, vol. 11, no. 5, pp. 40–48, Sep. 2024, DOI: 10.13718/j.cnki.jsjy.2024.05.005.
- [8] C. Mourning, H. Chenji, A. Hallman-Thrasher, S. Kaya, N. Abukamail, D. Juedes, and A. Karanth, "Reflections of cybersecurity workshop for K-12 teachers," in *Proc. 54th ACM Tech. Symp. Comput. Sci. Educ. (SIGCSE)*, New York, NY, USA, 2023, pp. 987–993. DOI: 10.1145/3545945.3569761
- [9] European Union Agency for Cybersecurity (ENISA), *ECSM 2022 Campaign Report*. Athens, Greece: ENISA, Mar. 2023, DOI: 10.2824/36758.
- [10] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165–176, May 2014, DOI: 10.1016/j.cose.2013.12.003.
- [11] Ministry of Education of the People's Republic of China, "Teacher digital literacy (industry standard)," Official Standard Document, 2022. [Online]. Available: https://www.moe.gov.cn/s78/A10/s5669/202203/t20220329_619320.html
- [12] Y. Cen, "Teacher digital literacy cultivation: Practical dilemmas and global actions," *Journal of Teacher Education*, vol. 11, no. 4, pp. 38–46, Jul. 2024, DOI: 10.13718/j.cnki.jsjy.2024.04.005.
- [13] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, vol. 91, no. 1, pp. 93–114, Jan. 1975. DOI: 10.1080/00223980.1975.9914308
- [14] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, Sep. 1989. DOI: 10.2307/249008
- [15] A. Pollini, T. C. Callari, A. Tedeschi, D. Ruscio, L. Save, F. Chiarugi, and D. Guerri, "Leveraging human factors in cybersecurity: An integrated methodological approach," *Cognition, Technology & Work*, vol. 24, no. 2, pp. 371–390, May 2022. DOI: 10.1007/s10111-021-00683-y
- [16] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, Feb. 1991. DOI: 10.1016/0749-5978(91)90020-T
- [17] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1986.
- [18] R. Ravichandran, S. Singh, and P. Sasikala, "Exploring school teachers' cyber security awareness, experiences, and practices in the digital age," *Journal of Cybersecurity Education, Research and Practice*, vol. 2025, no. 1, pp. 1–27, Jan. 2025. DOI: 10.62915/2472-2707.1214
- [19] O. S. Ahmed, A. Z. Al Rawashdeh, A. R. Al Arab, A. S. Ahmed, S. A. Nasef, and E. M. Abd elrahman, "The impact of school teachers awareness of student cyber security," *Pakistan Journal of Life and Social Sciences*, vol. 22, no. 2, pp. 17371–17380, 2024, DOI: 10.57239/PJLSS-2024-22.2.001264.
- [20] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber security awareness campaigns: Why do they fail to change behaviour?," in *Proc. Int. Conf. Cyber Security for Sustainable Society (CSSS)*, Coventry, U.K., 2015, pp. 118–131.