2023-08-24

An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work

Salamah F. Ben

Marco A. Palomino *School of Engineering, Computing and Mathematics*

Matthew J. Craven *School of Engineering, Computing and Mathematics*

Maria Papadaki

Steven Furnell *School of Engineering, Computing and Mathematics*

Recommended Citation

Ben, S. F., Palomino, M., Craven, M., Papadaki, M., & Furnell, S. (2023) 'An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work', *Applied Sciences*, 13(17), pp. 9595-9595. Available at: https://doi.org/10.3390/app13179595

applied sciences

MDPI

Article

An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work

Fai Ben Salamah [1,*], Marco A. Palomino [1,*], Matthew J. Craven [1], Maria Papadaki [2] and Steven Furnell [3]

[1] School of Engineering, Computing and Mathematics, University of Plymouth, Plymouth PL4 8AA, UK; matthew.craven@plymouth.ac.uk

[2] School of Computing and Engineering, University of Derby, Derby DE22 1GB, UK; m.papadaki@derby.ac.uk

[3] School of Computer Science, University of Nottingham, Nottingham NG8 1BB, UK; steven.furnell@nottingham.ac.uk

[*] Correspondence: fai.bensalamah@plymouth.ac.uk (F.B.S.); marco.palomino@plymouth.ac.uk (M.A.P.)

Abstract: Formalizing the approach towards risk management on social media is critical for organizations. Regrettably, a review of the state-of-the-art on cybersecurity training highlighted that the existing frameworks are either too generic or too cumbersome to be adapted to different organizations and needs. Thus, we developed the Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR), a framework that incorporates social media cybersecurity policies and best practices. The ACSTF-SMR enables organizations, trainers, and policymakers to address the challenges posed by social media in a way that satisfies employees' training needs and adjusts to their preferences. We tested the ACSTF-SMR with 38 case studies. Employees' behaviors, learning, and responses after training were assessed, and feedback was gathered to improve the framework. Interviews with policymakers were held to gain insight into the enforcement of social media policies. We conclude that the ACSTF-SMR is a reliable option to mitigate social media threats within organizations.

Keywords: cybersecurity; adaptive training; social media; education

check for updates

Citation: Ben Salamah, F.; Palomino, M.A.; Craven, M.J.; Papadaki, M.; Furnell, S. An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work. *Appl. Sci.* **2023**, *13*, 9595. https://doi.org/10.3390/app13179595

Academic Editors: Juan-Carlos Cano and Gianluigi Ferrari

Received: 18 July 2023
Revised: 9 August 2023
Accepted: 23 August 2023
Published: 24 August 2023

1. Introduction

Social media has transformed the communication landscape, although this has been at the expense of imminent dangers. Given that social media is based on the notion of community and relationships, its very nature means that users are expected to trust in each other and interact. Unfortunately, uncontrolled trust and thoughtless interaction may lead to vulnerabilities, which are often exploited by hackers [1,2].

Researchers have argued that most organizational incidents result, either directly or indirectly, from human errors, and this seems to be the case for cybersecurity incidents too [3–5]—according to the *2020 Data Breach Investigations Report*, humans play an important part in cyber threats [6]. Regrettably, the awareness of cybersecurity threats seems relatively low, particularly in relation to social media.

Employees need to learn how much information they can share on social media without taking unacceptable risks for the organizations for which they work [7–10]. Improving the security and privacy of employees on social media is vital, and such improvements must match the continuous evolution of technology [9]. Social media was not designed with built-in defenses [11]; therefore, its users are easy targets [12].

Many organizations have chosen to cope with social media risks in a reactive manner, rather than proactively controlling them [13]. Typically, social media policies are in place in organizations [14], although such policies do not necessarily seek to raise the awareness of the employees [15].

Although employee awareness is the first line of defense for information systems [12], the existing training approaches do not consider the awareness of different types of employees and different levels of understanding. Moreover, pondering the effects of human factors while developing mitigation strategies to prevent cybersecurity risks is not common [16]. One of the contributions of this paper is that it fills the resulting knowledge gap of identifying human factors that are responsible for aggravating cyber risks while using social media and providing an adaptable training framework to improve the knowledge and skills of the employees in organizations that use social media.

Many cybersecurity training frameworks face issues due to the trainees' perceptions. The training and instructional materials on awareness, or any other cybersecurity topic within an organization, rarely consider the employees' preferences for learning styles [2,17,18]. In fact, organizational training frameworks are often perceived as time-consuming, non-inviting, or intimidating. We intend to alleviate these issues by creating a framework that takes into account the preferences of the employees. However, we must start by identifying such preferences, so that we can offer a proper mix of delivery approaches; this has been deemed to be not only advisable but indispensable [19–21]. We propose the development of a new training framework such as the one suggested by Creswell [22], which can be used to test our ideas, collect research data, and examine various hypotheses. Our work makes the following contributions:

- A framework to develop cybersecurity training that is adaptable to the needs and preferences of different employees within an organization;
- A single and simple online guide to social media policies and the best security practices for organizations;
- A collection of compliance reports considering employee risk levels to support mitigation strategies.

This paper is organized as follows. Section 2 introduces the background for our work by providing a review of previous work and a comparison between the existing approaches and what we have done. Section 3 presents the framework methodology, which extends the methodology proposed by Schürmann et al. [20]. Section 4 includes an evaluation of our framework (ACSTF-SMR). Section 5 discusses training and social media policies from the perspective of policymakers. This is largely to fill the gap between the literature and practical experience. We complemented our work with 11 semi-structured interviews with policymakers who are involved in cybersecurity education and organizational training. Finally, Section 6 presents our conclusions.

2. Background

Previous studies have found that human factors—such as age, education, job role, behavior, and attitudes—affect an employee's awareness of cyberattacks within the organizations they work. Thus, we started our investigation by looking at the research on human factors that had been carried out before. Table 1 summarizes our findings from the existing literature. Afterwards, we present a detailed description of how our work compares to former developments.

Table 1. Findings linking cyber threats with human factors.

Age
Younger employees have a higher chance of being victims of cyberattacks than older peers [23,24].
Cybersecurity training is more vital for older people than younger peers [25,26].
People between 18 and 25 are more exposed to social media phishing than others [27].
Background
Employees with technological backgrounds are more familiar with cyber threats than others [28].
Job Role and Sectors
Job roles are a vital factor associated with cybersecurity risks [29].
Healthcare employees—doctors, nurses, and managers—face higher risks than others [30].
The financial sector is the most frequent target of cyberattacks [31].

Table 1. *Cont.*

Behavior and Attitudes
People who use social media for exchanging information are more likely to be victims of cyberattacks [32].
People who ignore security-related warnings are more likely to be victims of cyberattacks [23].

To compare our work with former developments, we have produced Table 2, which offers more details of the advantages provided by the existing approaches, their drawbacks, and how our work compares to them.

Table 2. Comparison with previous work.

Age	
Advantages	**Drawbacks**
Furnell and Vasileiou [33] have argued that the training must vary according to the age of the trainees because different age groups have varying preferences and levels of understanding of cybersecurity.	Furnell and Vasileiou did not study the problem specifically within the context of organizations with a presence and operations on social media, which is what we intend to do.
Hadlington [23] suggests that younger people are more vulnerable to phishing attacks than older ones.	Although we agree with Hadlington, we have not limited our analysis to phishing attacks, and we attempt to correlate different age ranges with other cybersecurity issues that are also part of social media.
Background	
Benefits	**Drawbacks**
A person's individual background and prior work experience play a vital role when addressing cybersecurity risks, as stated by Hatzivasilis et al. [24].	There was no previous study of the impact on cybersecurity of the background and work experience of employees enrolled in various sectors of the industry. This is what we have done, and what we encourage other researchers to do in the future.
Job Role and Sectors	
Benefits	**Drawbacks**
Nifakos et al. [30] argued that healthcare professionals—such as doctors, nurses, and medical support staff—pose higher risks to their organizations when they interact with social media platforms.	While we generally agree with Nifakos et al.'s observations [30]; healthcare is not the only sector in the industry that is at risk on social media. We are also interested in other sectors. Thus, we collected information from employees working in a wide range of organizations performing many different roles. We found that employees working in financial operations face a very high risk level [34], which agrees with recent estimates that the financial sector is the preference of choice for attackers—44% of the cyberattacks occur within the financial sector [31].

The present investigation involves a comprehensive review of the frameworks found in the literature. The objective is to critically evaluate these frameworks to come up with an optimal solution for the creation of an adaptive training strategy. As a result of the scarcity of research that accounts for human factors in cybersecurity, our review is confined to the cybersecurity training models presented in Table 3.

Table 3. Advantages and disadvantages of existing frameworks.

Framework/Model	Pros	Cons
Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity [2]	The consideration of human factors in cybersecurity is of the utmost importance, necessitating regular assessments of employees to ensure their sustained knowledge in this domain.	The primary emphasis of this framework is a broad understanding, rather than focusing on awareness inside the realm of social media.
Competency Development and Assessment Framework [35]	When providing cybersecurity training, it is crucial to consider the various roles performed by every employee within the organization and to consistently prioritize evaluation.	The assessment was conducted using a singular training methodology (namely, the "capture the flag" game).
Mission Cybersecurity Framework [36]	The significance of prioritizing policies as a foundational element for training.	The framework provided is rather broad and needs a specific emphasis on promoting awareness regarding social media.
Holistic Cybersecurity Maturity Assessment Framework [37]	A comprehensive analysis of the process involved in designing and implementing web-based evaluations, with a specific focus on their use as a benchmark for decision-making purposes.	The framework needed to adequately account for the distinctiveness of social media users at work concerning the organizational context.
TET Framework [38]	Prior to developing a successful cybersecurity training program, it is imperative to start with an evaluation of the individual employee's knowledge.	The approach does not fully account for employees' perceptions, attitudes, and preferences for training.
Cybersecurity awareness [39]	When developing cybersecurity training programs, it is essential to consider the learners' existing knowledge levels and human factors and emphasize behavior changes among the trainees.	The framework addresses concerns in a broad sense, with a specific focus on the capabilities and behaviors of trainees, although it does not consider social media risks.
Behavior Change Wheel Framework (BCW) [19]	Understanding the theoretical foundations of behavior change, identifying appropriate assessment methods, and ensuring the assessment is valid and reliable.	The validation was limited to the medical field and did not specifically address risks arising from social media.
Cybersecurity Culture Model [40]	This model aims to augment the comprehension and involvement of users in relation to cybersecurity policies, while considering a cybersecurity culture.	The framework places emphasis on the overarching culture of cybersecurity, without delineating any precise details of the approach.
NIST Framework [41]	Established standards, guidelines, and best practices in the field of security, with a primary objective of safeguarding critical infrastructure.	The framework disregards the influence of human factors in cybersecurity.
Social Media Risk Management Model [13]	A conceptual framework aimed at delineating and differentiating four key components of social media risk management.	The framework offers a broad perspective, rather than an adaptive training framework to enhance employee awareness.

The existing cybersecurity training frameworks for social media are largely generic, and in some cases cumbersome to implement. It is debatable if such frameworks can be adapted for all employees, considering their varying levels of knowledge, backgrounds, and preferences. While the *European Union Agency for Cybersecurity* (ENISA) has recommended a framework that considers human aspects [2], it primarily focuses on general awareness instead of social media awareness, which is what we intend to produce.

According to the ENISA [42], an effective cybersecurity training session should include an introduction, real-life stories, videos, games, group activities, and competition among learners. It is also important to include an analysis of real case studies and an explanation about why certain policies have been enacted. Avoiding technicisms and conveying short and clear messages are critical aspects too [43]. Bada and Nurse [15] have discussed the importance of training methods that are free of complexity and easy to comprehend—training simplicity leads to training success [44].

Brilingaite et al. [35] highlighted the importance of considering non-technical employees while selecting a training approach. However, their framework has limitations because it is based on gaming; hence, it may be appealing only to certain age brackets. Our framework stems from the need to consider different approaches, knowledge levels, and preferences, as highlighted previously by Salamah et al. [34].

Ki-Aries and Faily [45] carried out an experiment to ascertain people's preferences for video-based, game-based, or text-based training approaches. They found out that merging different approaches produces better outcomes than using only one. Thus, we aim to offer as many training options as possible, although we are aware of the complexities and demands of offering a variety of delivery methods in real-world scenarios [46].

Furnell and Vasileiou claimed that training is more effective when employees feel that it is tailored to them [33]. Therefore, training should be customized to organizations and circumstances [47], such as business needs, budgets, missions, and cultures [15]. That is exactly what we want to do, although in the context of social media risks, which has not been contemplated in detail in previous work.

Cybersecurity training needs to be based on the roles of the employees and their responsibilities within the organization [24]. However, the depth of the training may vary, as some employees need only basic knowledge and others need a thorough understanding. Hence, our framework begins with the identification of the requirements for training.

Demek et al. [13] argued that employees need to be trained thoroughly on cyber policies, and these policies need to be clear and easily enhance their effectiveness. Thus, as we will discuss later, our framework is based on simple and unambiguous questions derived from recommended policies and best practices.

Dawson [36] also highlighted the importance of policies in cybersecurity. Nevertheless, Dawson's framework is too generic and does not focus on human aspects [36]. Aliyu et al. [37] presented a cybersecurity assessment tool for higher education institutes but failed to consider the employees separately from the organization. As opposed to Aliyu et al. [37], we intend to prioritize the individuals and concentrate on social media.

Zhang et al. [21] pointed out that cybersecurity training is a long-term investment, and organizations must make sure that it does not become generic. Individual employees have different responsibilities within the organization [34], and their cybersecurity awareness and knowledge levels vary too. Although it is commonly accepted that one-size-fits-all training approaches fail [21], few studies have looked at how the training should be tailored in the context of social media, which is what this study aims to accomplish.

Among the existing frameworks to raise cybersecurity awareness, the study by Wang et al. [36] deserves careful consideration. Wang et al. [36] believe that training should be based on the employees' knowledge. Whilst we agree with this, we also think that the training needs to be based on the employees' preferences, perceptions, attitudes, and demographics.

Attention needs to be paid to the trainers too. The trainers play a huge role in increasing the enthusiasm towards the learning process [35]. Indeed, the ENISA has worked on enhancing network security by raising the knowledge of the trainers [48]. Researchers argue that having qualified and skilled trainers is a must [49].

Regarding testing and evaluation, Alshaikh et al. [19] validated their work in the medical domain, although we will validate our work in other industries too, such as the financial sector, and we have collected information from employees in various organizations.

3. Methods

The ACSTF-SMR follows the methodology proposed by Schürmann et al. [20], which defines the three fundamental steps for cybersecurity training. The first step consists of analyzing the target group to identify their roles and responsibilities. The second step involves risk assessment, and the third step identifies gaps and vulnerabilities. The development of the training material and the evaluation of the training program are additional steps that complete the entire process.

Taking Schürmann et al. [20] as our starting point, we propose a training framework consisting of four steps, as shown in Figure 1. Our first step identifies the target audience—employees' backgrounds are determined here, including their job roles, age, education, work experience, and patterns of social media usage. We will consider the employees' preferred training methods to ensure our training is adaptable [34].

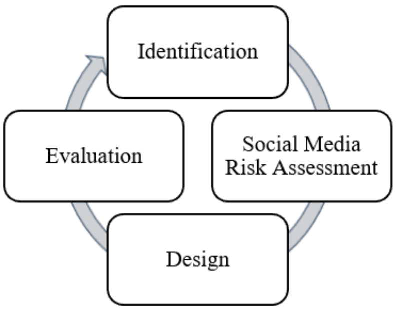

Figure 1. The Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR).

The communication with the employees, the quizzes, and the training were all carried out in the English language. Due to the nature of our investigation and given that we were required to store and analyze details about the employees' work and their demographics, we had to undertake the ethical review process stipulated by the University of Plymouth (Plymouth, UK), which is where we were based while conducting our research.

The ethical review was recorded through the Plymouth Ethics Online System (PEOS) (Plymouth, UK) [50], and the approval was granted on 5 September 2020. Abiding by the University of Plymouth's ethical approval policy, the survey to gather information about the participants was conducted in anonymity.

The thirteen training approaches that we offered to the employees are listed in Table 4. We provided a wide range of options to cater for as many preferences as possible.

Table 4. Training options.

Training Option	Description
Awareness Raising Events	Occasional events at which employees are invited to increase their awareness and knowledge of cybersecurity risks on social media.
Email	Messages sent from management or training coordinators to the employees to deliver cybersecurity information, warnings about new or specific threats, etc.
Games	Software or classroom games that facilitate engagement and participation.
Incentives	Concessions or benefits offered to promote "good" behavior and discourage "bad" behavior.
Mock Attacks	Training which imitates various forms of cyberattacks as a way of preparation. Cyberattacks may include phishing tests, sharing virus-infected devices, etc.

Table 4. *Cont.*

Training Option	Description
Online Training Course	Training which can be attended individually at convenient times.
Posters	Large printed pictures that include tips on useful resources, overviews of threats, information about new risks, advice, and suitable contacts within the organization.
Social Media Posts	Alerts posted on social media platforms about specific threats, good practices, and useful resources.
Stories	Real-life stories that can be printed on flyers, told in videos, or during online sessions.
Tip Sheets	Short lists providing easy access to key information about cybersecurity.
Videos	Recordings featuring references to good practice to demonstrate correct responses to cyber threats.
Webinars	A seminar conducted over the Internet, which can be recorded and saved in an accessible place—for example, the organization's Intranet for those who could not attend or want to revisit aspects of the talk.
Workshop	In-class training where the employees interact with others and ask questions.

Our second step evaluates the risk levels of each individual employee following the recommendations of the National Cyber Security Centre (NCSC) [51] and its best practices for social media [52]. To do so, employees take a quiz to assess their knowledge and skills, and we collect the data that we use to determine what sort of training is needed and how it will be delivered.

Using a risk assessment tool is a cornerstone of our framework. Our risk assessment tool is based on two main factors, the *target group* (TG) and *awareness* (A). To explore the awareness factors, the questions in our quiz assess the employees' level of knowledge regarding best practices for social media. The quiz is designed to estimate the three security risk awareness levels: *high*, *moderate*, and *low* [20]. The parameters used to develop the quiz are listed below:

- Hacking challenges;
- Privacy and security;
- Password protection;
- Identification of phishing;
- Incident report;
- Two-factor authentication.

An organization's training program will be based on the *awareness scores* that the employees are awarded. An awareness score indicates how much knowledge an employee has of social media best practices. The score is made up of three components:

- Knowledge: The knowledge of the employee about safe behavior on social media;
- Behavior: The behavior of the employee in response to cybersecurity incidents;
- Attitude: The attitude of the employee about the importance of following the best practices recommended.

To calculate the score for each employee, the quiz includes ten generic cybersecurity questions and five questions for each independent social media platform—five questions for Facebook, five for Instagram, and so on. Employees select the questions they answer based on their social media needs within their organizations—for instance, some employees may only use Facebook, whereas others may combine Facebook with Instagram.

The design is our third step, as indicated in Figure 1. The design involves the creation of a training program that respects the employees' preferences and fulfills their needs for knowledge, behavior, and attitude improvement. This is the main difference between our work and other existing frameworks [13,36,38]. This is the step where we can make use of human factors that we have identified as responsible for aggravating cyber risks and suggest mitigation strategies. This is also the step where we can cater for the employees' preferences and learning styles.

Finally, the fourth step of our proposed framework consists of evaluating the adaptive cybersecurity training program designed in the previous step, based on all of the information collected so far. After the training has taken place, we will gather feedback about the training materials and delivery, so that we can make improvements.

3.1. Validation Strategies

A framework's validity is established when it effectively achieves its objectives [53,54]. To verify that the ACSTF-SMR has achieved its objectives, we employ case studies, surveys, and interviews.

3.1.1. Case Studies

Case studies are guiding tools for identifying issues observed in actual scenarios [55]. Our suggested framework has been tested empirically through case studies to find evidence to support the outcomes of a training program. The ACSTF-SMR has been applied to various employees with different roles and backgrounds in Kuwaiti organizations that form parts of our case studies.

Even though we only obtained information from Kuwaiti employees, Kuwait's conditions helped us acquire a thorough understanding of some of the global cybersecurity issues. Kuwait is among the five Arab countries that use social media the most [56]. In addition, it is ranked eighth for email hacking and sixth for spam attacks [57]. Thus, focusing on Kuwait's case can provide us with invaluable insight into cybersecurity issues in Arab nations and globally.

3.1.2. Survey and Interviews

An online survey was conducted to get employees' feedback on the training program's structure and content. The survey concluded with open-ended questions to provide employees with an opportunity to expand further on their comments or clarify their views. Moreover, the trainer also recorded the employees' reactions during the training sessions that were organized online.

To avoid falling into the trap of basing business decisions on skewed survey results, we prevented selection and response bias in the following ways [58]:

- Selection bias: We gathered feedback from all those involved in our training program, namely the employees who were included in the study, the training providers, and the policymakers. This meant that no group was left out of the survey, which addressed any possible sampling bias. Additionally, we asked everyone to take our survey immediately after the training was completed, while they could still recall their experience. Given that we received answers from all the stakeholders involved—this was encouraged by ensuring everyone that the survey was anonymous—we can confirm that a non-response bias did not affect our analysis either.
- Response bias: To prevent acquiescence bias, we avoided questions that only allow a "yes" or "no" answer because they do not provide sufficient levels of nuance. Instead, we employed a Likert response scale that does not lend itself easily to acquiescence bias [59]. Employees were asked to rate our different training components on a scale of 1 to 5 and to indicate their agreement with some statements about the training program.

3.1.3. Validation Process

To validate the ACSTF-SMR, we separated the employees into two groups: the first group received customized training and the second group received standard training. After the training was completed, we reassessed the employees' awareness.

We evaluated the outcomes of the training program. A statistical *t*-test [60] was used to determine if the training achieved its purpose. Additional questions asked after completing the training were designed to gain feedback and improve future delivery.

4. Results

An invitation was sent by email to 250 employees working across various industries in Kuwaiti organizations to participate in an experimental study where we offered to train employees on cybersecurity risks present on social media. The text of the invitation included information about the training that we were providing, how long it would take to complete it, and their right to withdraw from the study at any time.

A total of 80 employees out of the 250 who received our invitation responded and completed the initial evaluation. Once the initial evaluation was submitted and we had returned to the respondents a report stating how proficient they were on the use of social media at work, we invited them to join our training. Only 38 of them agreed to be trained. Table 5 provides information about the 38 employees who received our training.

Table 5. Background of the participants of our study.

ID	Industry	Gender	Age	Educational Stage	Experience
1	Business/Administration	M	34	Bachelor's	9
2	Education/Military	M	55+	Postgraduate	25+
3	Art/Entertainment	M	43	Postgraduate	20
4	Education	F	40	Postgraduate	15
5	Management/Business	F	36	Bachelor's	13
6	Education/Administration	M	29	Bachelor's	7
7	IT	M	39	Bachelor's	18
8	Business/Financial	F	44	Bachelor's	22
9	Business/Financial	M	46	Bachelor's	22
10	Administration	M	33	Secondary	5
11	Management	F	30	Bachelor's	8
12	Administration	M	35	Secondary	6
13	Administration	F	26	Primary	1
14	Military	M	40	Bachelor's	16
15	Administration	M	44	Primary	20
16	Military	M	38	Postgraduate	17
17	Administration	F	26	Bachelor's	3
18	Management	F	49	Postgraduate	22
19	IT	F	41	Bachelor's	18
20	Management	F	32	Postgraduate	10
21	Education	M	48	Postgraduate	15
22	IT	F	36	Postgraduate	13
23	Management	F	43	Bachelor's	22
24	IT	M	31	Bachelor's	5

Table 5. *Cont.*

ID	Industry	Gender	Age	Educational Stage	Experience
25	Education	F	45	Bachelor's	17
26	Art/Entertainment	F	33	Bachelor's	6
27	Administration	F	39	Postgraduate	6
28	IT	M	29	Bachelor's	5
29	Military	M	42	Postgraduate	24
30	Education	M	32	Postgraduate	7
31	Business/Financial	M	31	Bachelor's	11
32	Education	M	35	Bachelor's	8
33	Business/Financial	M	35	Postgraduate	15
34	Military	M	40	Bachelor's	20
35	Military	M	37	Bachelor's	17
36	Education	F	38	Postgraduate	15
37	Administration	F	38	Primary	12
38	Management	M	30	Bachelor's	5

The 38 participants were offered the choice to receive the type of training that they wanted, and they were split into two groups. The first group consisted of 24 people, and they were given customized training. The remaining 14 were included in the second group and were provided with standard training.

4.1. Customized Training

To accommodate for all participants' needs and preferences, 24 customized training sessions were designed. A total of 11 of the 24 participants who preferred customized training sessions chose to attend in person, while 12 of them preferred to watch videos in their own time to improve their skills. Each video lasted between 5 and 8 min and showed graphs, images, and brief descriptions to explain common risks and errors committed while working on social media platforms.

Only one of the 24 participants chose to learn through posters, and posters were created for her. However, owing to the restrictions imposed by the COVID-19 pandemic, the 11 participants who chose to attend the sessions in person had to attend them virtually in the end. The virtual training sessions were conducted via Zoom, the online meeting platform (https://zoom.us/ accessed on 21 August 2023).

The customized training sessions increased the cybersecurity knowledge and skills of all participants. The types of training preferred by the participants, the types of training that we delivered, and the pre- and post-training scores are all shown in Table 6. It should be noted that the quiz for some employees was longer than for others because some employees required training for more than one social media platform.

A statistical *t*-test [60] was performed to further compare the two groups—pre- and post-training. The confidence intervals for the two groups were set to 95% and 99%, respectively, which meant that *p*-values between 0.05 and 0.01, respectively, were considered statistically significant. The *t*-test results demonstrate that the training sessions increased the cybersecurity knowledge and skills of the participants. The mean difference between the pre- and post-training scores was 6.54. Thus, we can confirm that after the training was delivered according to the employees' needs, preferences, and perceptions, their knowledge and skills increased. All scores are visually represented in Figure 2.

Table 6. Employees who participated in customized training.

Participant ID	Training Preferences	Delivery Mode	Pre-Training Score	Post-Training Score
1	Online Training + Workshops + Videos	Video	21 out of 25	24 out of 25
2	Workshops + Online Training	Virtual	7 out of 25	18 out of 25
3	Online Training	Virtual	13 out of 25	25 out of 25
4	Video + Workshops	Video	14 out of 20	19 out of 20
5	Online Training + Video + Workshops	Video	12 out of 20	17 out of 20
6	Video + Workshops	Video	11 out of 25	17 out of 25
7	Workshops	Virtual	11 out of 15	15 out of 15
8	Online + Posters + Tip sheets	Video	20 out of 25	24 out of 25
9	Workshops + Online Training + Videos	Virtual	11 out of 20	18 out of 20
10	Workshops + Posters	Virtual	11 out of 20	17 out of 20
11	Video + Games	Video	12 out of 20	20 out of 20
12	Workshops + Video + Workshops	Virtual	16 out of 25	23 out of 25
13	Video + Workshops + Games	Video	7 out of 15	12 out of 15
14	Workshops	Virtual	14 out of 25	23 out of 25
15	Videos	Video	5 out of 15	15 out of 15
16	Workshops + Videos	Video	10 out of 20	17 out of 20
17	Video + Posters + Workshops	Video	6 out of 15	14 out of 15
18	Online Training + Video + Workshops	Video	11 out of 20	20 out of 20
19	Workshops + Posters	Virtual	14 out of 20	20 out of 20
20	Workshops + Posters	Virtual	11 out of 20	19 out of 20
21	Workshops + Online Training + Games	Virtual	14 out of 20	19 out of 20
22	Workshops + Online Training + Posters	Virtual	14 out of 20	19 out of 20
23	Online + Workshops + Games	Video	12 out of 25	17 out of 25
24	Posters + Mock Attacks + Games	Posters	23 out of 25	25 out of 25

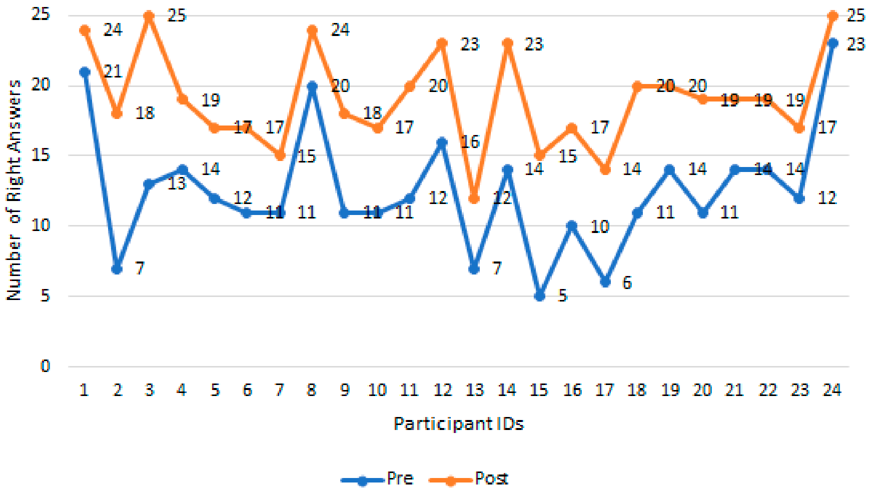

Figure 2. Scores for the employees who undertook customized training.

4.2. Standard Training

As stated earlier, 14 employees underwent a standard training program. This training also increased the knowledge and skills of the participants. However, the improvement after the training sessions was not as much as in the case of the customized training. The types of training preferred by the participants, the types of training that we delivered, as well as the pre- and post-training scores are all shown in Table 7. It should be noted that the quiz for some employees was longer than for others because some employees required training in more than one social media platform.

Table 7. Participants who undertook standard training.

Participant ID	Training Preferences	Delivery Mode	Pre-Training Score	Post-Training Score
25	Posters + Workshops + Tip Sheets	Video	8 out of 20	16 out of 20
26	Videos + Mock Attacks + Email	Posters	12 out of 15	12 out of 15
27	Online Training + Videos + Posters + Email	Tip-sheet	15 out of 20	15 out of 20
28	Social Media Posts	Tip-sheet	11 out of 15	11 out of 15
29	Workshops	Video	4 out of 15	3 out of 15
30	Workshops + Online Training + Mock Attacks	Video	16 out of 20	13 out of 20
31	Workshops + Videos + Social Media Posts	Tip-sheet	13 out of 20	17 out of 20
32	Workshops	Video	3 out of 20	6 out of 20
33	Videos + Games + Posts	Tip-sheet	12 out of 15	12 out of 15
34	Social Media Posts	Tip-sheet	9 out of 20	10 out of 20
35	Online Training	Tip-sheet	11 out of 15	11 out of 15
36	Workshops + Online Training + Videos	Tip-sheet	9 out of 25	15 out of 25
37	Games + Social Media Posts + Email	Video	9 out of 20	8 out of 20
38	Social Media Posts	Tip-sheet	9 out of 15	8 out of 15

A second *t*-test was performed to further compare the two groups—pre- and post-standard-training. The mean difference between the pre- and post-standard-training scores was 1.14. In other words, standard training was not particularly effective, and it failed to enhance the employees' knowledge in some cases, as shown in Figure 3.

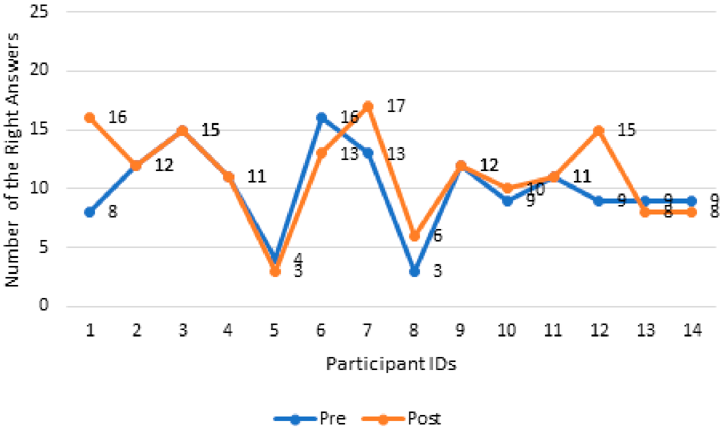

Figure 3. Scores of the employees who undertook standard training.

4.3. Training Feedback

Training effectiveness can be reliably estimated through feedback [61]. The employees' feedback indicates how satisfied they are with the training environment and the trainer's efficacy. Andriotis [62] emphasizes that the training feedback must be analyzed in terms of engagement, suggestions, comprehension, and effectiveness. Hence, we asked the employees the questions listed in Table 8; only anonymous feedback was accepted.

Table 8. Feedback questions.

Element	Question (s)
Effectiveness	• I am satisfied with the training session. • I would recommend this training program to others.
Comprehension	• The training motivates me to learn more about social media risks.
Attractiveness	• The training session accommodates my learning preferences.
Engagement	• I feel that the training was worth my time.
Suggestions	• What did you like the most about the training session? • What can be improved?

Most of the employees who undertook the customized training were positive towards the training program. A total of 96% of them stated that the training had motivated them to learn more about the risks on social media and the tools that keep them secure. They also showed eagerness to educate others. Overall, they were satisfied.

The open-ended questions at the bottom of Table 8 created qualitative datasets to validate our framework's effectiveness. This gave us more insight into the employees' perceptions and views. Examples of the answers received for the question "What did you like the most about the training session?" appear in Table 9.

Table 9. Customized training feedback.

What Did You Like the Most about the Training Session?
"I enjoyed how obvious and straightforward the subject is!"
"Information was provided simply and directly".
"Explaining my typical mistakes and teaching me to adopt best practices were the key strengths of the session".
"Receiving immediate feedback on my answers to the quiz is more beneficial than having to wait for the trainer to evaluate my responses and get back to me".
"It was exceptional for me".

One of the employees suggested uploading the videos to YouTube—the online video sharing platform (https://www.youtube.com/ accessed on 21 August 2023)—so that everyone can access them at any time. This shows how well received the training was and how much it is needed.

Some of the employees who undertook the standard training also provided us with feedback for the open-ended questions at the bottom of Table 8, and examples of this are shown in Table 10. Additionally, two of the employees who undertook the standard training admitted that they did not complete the program; apparently, they did not like the posters and ignore them.

Table 10. Standard training feedback.

What Did You Like the Most about the Training Session?
"More images and infographics are needed".
"Screenshots needed to be improved to show step-by-step the procedure we must follow".
"Quiz questions need to be clearer".

5. Discussion

To fill the gap between the literature and practical experience, we complemented our work with the employees with 11 semi-structured interviews with policymakers who are involved in cybersecurity education and organizational training.

Table 11 displays the background details of our interviewees, who came from different institutions in the state of Kuwait.

Table 11. Policymakers and cybersecurity educators' background details.

Interviewee ID	Education	Years of Experience
1	Master's	4
2	Bachelor's	2
3	PhD	10
4	PhD	21
5	Bachelor's	4
6	PhD	6
7	Master's	17
8	Bachelor's	13
9	PhD	3
10	PhD	18
11	Master's	16

As far as cybersecurity policies are concerned, our interviews allowed us to conclude that most organizations have such policies in place. However, they may not be clear about their significance in the context of social media. One of the interviewees told us, "Staff in my organization is totally in the dark". Another one said, "We are cautious about the secure use of the Internet, but hardly any policy is in place for social media".

Policymakers responsible for enforcing security policies have struggled with the mindsets of social media users. "Putting policies in place is itself a daunting task", was said by one of the senior security officers interviewed. Another one argued that "organizational risk is reduced significantly by applying policies strictly without exception". Therefore, some of the policymakers think social media policies must be enforced as part of job descriptions and contracts. Regardless, changing individuals' attitudes on social media is not simple, and our interviewees considered this "a global issue" not limited to Kuwait.

6. Conclusions

The framework provided here is a novel approach to generating adaptive cybersecurity training to mitigate social media risks within organizations. The framework starts by assessing an employee's level of awareness of social media threats, and then proceeds to increase their knowledge and skills. Our goal is to assist organizations in preventing and addressing social media cybersecurity-related risks.

While the framework's development is an ongoing process, it contributes to raising general awareness. Risk assessment tools can assist organizations in firmly establishing risk mitigation plans. Our Adaptive Cybersecurity Training Framework for Social Media Risks (ACSTF-SMR) provides a methodology for organizations, trainers, and policymakers to approach the challenges of social media cybersecurity training.

To determine the efficiency of the adaptive training, the employees were divided into two groups. The first group received customized training, whereas the second received standard training. The customized training took into account each employee's needs, preferences, views, and level of knowledge. The *t*-test was used to compare the results before and after training, revealing that customized training is superior to standard training.

The employees' feedback was collected by administering a questionnaire. We captured quantitative and qualitative feedback on the training program. Andriotis' evaluation approach was used to assess the feedback we received. The results establish that the ACSTF-SMR can mitigate social media threats in organizations.

While our study met its objectives, it had limitations that must be acknowledged. Human behavior is unpredictable and must be improved through training, as employees are the weakest link in cyberattacks. However, understanding human behavior as part of social media interactions in different geographical locations and different sociocultural backgrounds is a comprehensive task that cannot be approached in the short term. While this study provides the basis for future work, forthcoming research should confirm that the proposed framework can be validated in various geographies.

We emphasized respecting the preferences of employees. However, newcomers may not be able to make some choices simply because they are not acquainted with the different options. Thus, the future research should also focus exclusively on those with previous experience with more than one training method and find ways to identify why some methods are more adaptive than others.

Author Contributions: Conceptualization, M.A.P., M.P. and S.F.; Methodology, F.B.S. and M.A.P.; Software, F.B.S.; Validation, F.B.S.; Formal analysis, M.P.; Investigation, F.B.S. and M.A.P.; Data curation, F.B.S.; Writing—original draft, F.B.S. and M.A.P.; Writing—review & editing, M.A.P., M.J.C., M.P. and S.F.; Visualization, F.B.S.; Supervision, M.A.P., M.P. and S.F. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and approved by the Ethics Committee of the University of Plymouth (date of approval: 5 September 2020).

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The data presented in this study are available on request from the corresponding author. The data are not publicly available due to reasons of data protection.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Aldawood, H.; Skinner, G. Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and 326 Ongoing Issues. *Future Internet* **2019**, *11*, 73. [CrossRef]
2. European Network and Information Security Agency (ENISA). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. 2019. Available online: https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity (accessed on 21 August 2023).
3. Haeussinger, F.; Kranz, J. *Antecedents of Employees' Information Security Awareness-Review, Synthesis, and Directions for Future Research*; Association for Information Systems AIS Electronic Library: Athens, Greece, 2017.
4. Tsokkis, P.; Stavrou, E. A password generator tool to increase users' awareness on bad password construction strategies. In Proceedings of the 2018 International Symposium on Networks, Computers and Communications (ISNCC), Rome, Italy, 19–21 June 2018; pp. 1–5.

5. Jamil, A.; Asif, K.; Ghulam, Z.; Nazir, M.K.; Alam, S.M.; Ashraf, R. MPMPA: A mitigation and prevention model for social engineering-based phishing attacks on Facebook. In Proceedings of the 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 10–13 December 2018; pp. 5040–5048.
6. DBIR. Data Investigations Report 2020. *Tech. Rep. Verizon*. 2020. Available online: https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf (accessed on 21 August 2023).
7. Parsons, K.; McCormac, A.; Pattinson, M.; Butavicius, M.; Jerram, C. A study of information security awareness in Australian government organisations. *Inf. Manag. Comput. Secur.* **2014**, *22*, 334–345. [CrossRef]
8. Blackburn, J.; De Cristofaro, E.; Sirivianos, M.; Strufe, T. Cybersafety in modern online social networks (Dagstuhl reports 17372). In *Dagstuhl Reports*; Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik: Wadern, Germany, 2018; Volume 7.
9. Zhang, Z.; Gupta, B.B. Social media security and trustworthiness: Overview and new direction. *Future Gener. Comput. Syst.* **2018**, *86*, 914–925. [CrossRef]
10. Thakur, K.; Hayajneh, T.; Tseng, J. Cyber security in social media: Challenges and the way forward. *IT Prof.* **2019**, *21*, 41–49. [CrossRef]
11. Ferrara, E. The history of digital spam. *Commun. ACM* **2019**, *62*, 82–91. [CrossRef]
12. Herath, T.B.G.; Khanna, P.; Ahmed, M. Cybersecurity practices for social media users: A systematic literature review. *J. Cybersecur. Priv.* **2022**, *2*, 1–18. [CrossRef]
13. Demek, K.C.; Raschke, R.L.; Janvrin, D.J.; Dilla, W.N. Do organizations use a formalized risk management process to address social media risk? *Int. J. Account. Inf. Syst.* **2018**, *28*, 31–44. [CrossRef]
14. Banghart, S.; Etter, M.; Stohl, C. Organizational boundary regulation through social media policies. *Manag. Commun. Q.* **2018**, *32*, 337–373. [CrossRef]
15. Bada, M.; Nurse, J.R. Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Inf. Comput. Secur.* **2019**, *27*, 393–410. [CrossRef]
16. King, Z.M.; Henshel, D.S.; Flora, L.; Cains, M.G.; Hoffman, B.; Sample, C. Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Front. Psychol.* **2018**, *9*, 39. [CrossRef]
17. Christopher, L.; Choo, K.-K.; Dehghantanha, A. Honeypots for employee information security awareness and education training: A conceptual easy training model. In *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*; Elsevier: Amsterdam, The Netherlands, 2017; pp. 111–129.
18. Caulkins, B.D.; Badillo-Urquiola, K.; Bockelman, P.; Leis, R. Cyber workforce development using a behavioral cybersecurity paradigm. In Proceedings of the 2016 International Conference on Cyber Conflict (CyCon US), Washington, DC, USA, 21–23 October 2016; pp. 1–6.
19. Alshaikh, M.; Naseer, H.; Ahmad, A.; Maynard, S.B. Toward Sustainable Behaviour Change: An Approach for Cyber Security Education Training and Awareness. In Proceedings of the 27th European Conference on Information Systems (ECIS), Stockholm & Uppsala, Sweden, 8–14 June 2019.
20. Schürmann, C.; Jensen, L.H.; Sigbjörnsdóttir, R.M. Effective cybersecurity awareness training for election officials. In *International Joint Conference on Electronic Voting*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 196–212.
21. Zhang, Z.J.; He, W.; Li, W.; Abdous, M. Cybersecurity awareness training programs: A cost–benefit analysis framework. *Ind. Manag. Data Syst.* **2021**, *121*, 613–636. [CrossRef]
22. Creswell, J.W. A Framework for Design. In *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*; Laughton, C.D., Ed.; SAGE Publications: London, UK, 2003; pp. 3–26.
23. Hadlington, L. Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. *Int. J. Cyber Criminol.* **2018**, *12*, 262–274.
24. Hatzivasilis, G.; Ioannidis, S.; Smyrlis, M.; Spanoudakis, G.; Frati, F.; Goeke, L.; Hildebrandt, T.; Tsakirakis, G.; Oikonomou, F.; Leftheriotis, G.; et al. Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Appl. Sci.* **2020**, *10*, 5702. [CrossRef]
25. Saridakis, G.; Benson, V.; Ezingeard, J.N.; Tennakoon, H. Individual Information Security, User Behaviour and Cyber Victimisation: An Empirical Study of Social Networking Users. *Technol. Forecast. Soc. Chang.* **2016**, *102*, 320–330. [CrossRef]
26. Blackwood-Brown, C.; Levy, Y.; D'Arcy, J. Cybersecurity Awareness and Skills of Senior Citizens: A Motivation Perspective. *J. Comput. Inf. Syst.* **2021**, *61*, 195–206. [CrossRef]
27. Parker, H.J.; Flowerday, S.V. Contributing Factors to Increased Susceptibility to Social Media Phishing Attacks. *S. Afr. J. Inf. Manag.* **2020**, *22*, 1–10. [CrossRef]
28. Gasiba, T.; Lechner, U.; Pinto-Albuquerque, M. CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments. In Proceedings of the International Conference on Business Information Systems; Springer: Berlin/Heidelberg, Germany, 2021; pp. 370–387.
29. Toth, P.; Klein, P. A Role-Based Model for Federal Information Technology/Cyber Security Training. *NIST Spec. Publ.* **2013**, *800*, 1–152.
30. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review. *Sensors* **2021**, *21*, 5119. [CrossRef]

31. Pedley, D.; Borges, T.; Bollen, A.; Shah, J.N.; Donaldson, S.; Furnell, S.; Crozier, D. Cyber Security Skills in the UK Labour Market 2020. 2020. Available online: https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020 (accessed on 21 August 2023).
32. Van Schaik, P.; Jansen, J.; Onibokun, J.; Camp, J.; Kusev, P. Security and Privacy in Online Social Networking: Risk Perceptions and Precautionary Behaviour. *Comput. Hum. Behav.* **2018**, *78*, 283–297. [CrossRef]
33. Furnell, S.; Vasileiou, I. Security education and awareness: Just let them burn? *Netw. Secur.* **2017**, *2017*, 5–9. [CrossRef]
34. Ben Salamah, F.; Palomino, M.A.; Papadaki, M.; Furnell, S. The Importance of the Job Role in Social Media Cybersecurity Training. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 6–10 June 2022; pp. 454–462. [CrossRef]
35. Brilingaite, A.; Bukauskas, L.; Juozapavicius, A. A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Secur.* **2020**, *88*, 101607. [CrossRef]
36. Dawson, M. Applying a holistic cybersecurity framework for global it organizations. *Bus. Inf. Rev.* **2018**, *35*, 60–67. [CrossRef]
37. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
38. Wang, Y.; Qi, B.; Zou, H.-X.; Li, J.-X. Framework of raising cyber security awareness. In Proceedings of the 2018 IEEE 18th International Conference on Communication Technology (ICCT), Chongqing, China, 8–11 October 2018; pp. 865–869.
39. Rieff, I. Systematically applying gamification to cyber security awareness trainings: A framework and case study approach. Master's Thesis, Delft University of Technology, Delft, The Netherlands, 2018.
40. Georgiadou, A.; Mouzakitis, S.; Bounas, K.; Askounis, D. A cyber-security culture framework for assessing organization readiness. *J. Comput. Inf. Syst.* **2022**, *62*, 452–462. [CrossRef]
41. Barrett, M.P. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. 2018. Available online: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 (accessed on 21 August 2023).
42. European Union Agency for Cybersecurity. Good Practice Guide on Training Methodologies. 2014. Available online: https://www.enisa.europa.eu/publications/good-practice-guide-on-training-methodologies/ (accessed on 21 August 2023).
43. Ghafir, I.; Saleem, J.; Hammoudeh, M.; Faour, H.; Prenosil, V.; Jaf, S.; Jabbar, S.; Baker, T. Security threats to critical infrastructure: The human factor. *J. Supercomput.* **2018**, *74*, 4986–5002. [CrossRef]
44. Kraus, L.; Švábenský, V.; Horák, M.; Matyás, V.; Vykopal, J.; Celeda, P. Want to Raise Cybersecurity Awareness? Start with Future IT Professionals. In Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1, Turku, Finland, 7–12 July 2023.
45. Ki-Aries, D.; Faily, S. Persona-centred information security awareness. *Comput. Secur.* **2017**, *70*, 663–674. [CrossRef]
46. Nicholson, D.; Massey, L.; O'Grady, R.; Ortiz, E. Tailored cybersecurity training in LVC environments. In Proceedings of the MODSIM World Conference, Virginia Beach, VA, USA, 19 May 2016.
47. Glaspie, H.W.; Karwowski, W. Human factors in information security culture: A literature review. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, Los Angeles, CA, USA, 17–21 July 2017; pp. 269–280.
48. European Network and Information Security Agency (ENISA). Collaborative Solutions for Network Information Security in Education. 2012. Available online: https://www.enisa.europa.eu/publications/ (accessed on 21 August 2023).
49. Javidi, G.; Sheybani, E.; Pieri, Z. A holistic approach to k12 cybersecurity education. In Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS), Las Vegas, NV, USA, 29 July–1 August 2019; pp. 77–80.
50. University of Plymouth. Plymouth Ethics Online System (PEOS). 2022. Available online: https://www.plymouth.ac.uk/research/plymouth-ethics-online-system (accessed on 21 August 2023).
51. NCSC. The National Cyber Security Centre. 2023. Available online: https://www.ncsc.gov.uk/ (accessed on 21 August 2023).
52. NCSC. Social Media: How to Use It Safely. 2019. Available online: https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely#:~:text=Use (accessed on 21 August 2023).
53. Ostroff, C. Training effectiveness measures and scoring schemes: A comparison. *Pers. Psychol.* **1991**, *44*, 353–374. [CrossRef]
54. Holgado Tello, F.P.; Chacon Moscoso, S.; Barbero Garcia, I.; Sanduvete Chaves, S. Training satisfaction rating scale: Development of a measurement model using polychoric correlations. *Eur. J. Psychol. Assess.* **2006**, *22*, 268–279. [CrossRef]
55. Yin, R.K. *Case Study Research: Design and Methods*; Sage: Washington, DC, USA, 2009; Volume 5.
56. Alansari, M.M.; Aljazzaf, Z.M.; Sarfraz, M. On Cyber Crimes and Cyber Security. In *Developments in Information Security and Cybernetic Wars*; IGI Global: Hershey, PA, USA, 2019; pp. 1–41.
57. Cleary, G.; Corpin, M.; Cox, O. *Symantec Internet Security Threat Report*; Technical Report 23; Symantec Corporation: Mountain View, CA, USA, 2018. Available online: https://docs.broadcom.com/doc/istr-23-executive-summary-en (accessed on 21 August 2023).
58. Hudson, D.; Seah, L.H.; Hite, D.; Haab, T. Telephone presurveys, self-selection, and non-response bias to mail and internet surveys in economic research. *Appl. Econ. Lett.* **2004**, *11*, 237–240. [CrossRef]
59. Joshi, A.; Kale, S.; Chandel, S.; Pal, D.K. Likert scale: Explored and explained. *Br. J. Appl. Sci. Technol.* **2015**, *7*, 396. [CrossRef]
60. Kim, T.K. T test as a parametric statistic. *Korean J. Anesthesiol.* **2015**, *68*, 540–546. [CrossRef] [PubMed]

61. Velada, R.; Caetano, A. Training transfer: The mediating role of perception of learning. *J. Eur. Ind. Train.* **2007**, *31*, 283–296. [CrossRef]
62. Andriotis, N. Elements to Include in any Post Training Evaluation Questionnaire. eFront Blog. 2019. Available online: https://www.efrontlearning.com/blog/2017/12/element-post-evaluation-training-questionnaire.html (accessed on 14 May 2023).

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.