Measuring Cybersecurity Teaching: Case University Students in Finland

Tiina Schafeitel-Tähtinen*, Jukka Koskinen, and Marko Helenius

Faculty of Information Technology and Communication Sciences, Tampere University, Tampere, Finland
Email: tiina.schafeitel-tahtinen@tuni.fi (T.S.-T.); jukka.koskinen@tuni.fi (J.K.); marko.helenius@tuni.fi (M.H.)
*Corresponding author

***Abstract*—We present effectiveness measurements of five cybersecurity teaching interventions. We created a model for examining dependencies between teaching, students' self-perceived cybersecurity knowledge and skills, cybersecurity related interests, attitudes, and self-efficacy, and intended and recalled security behaviour. We tested the model hypotheses and measured differences between before and after receiving teaching. We found teaching has moderate to strong positive correlations with knowledge, and skills, as well as topic, further studies, and career interests. Students with higher cybersecurity specific self-efficacy have a higher interest towards intervention topics, further cybersecurity studies, cybersecurity career, and cybersecurity research. Self-efficacy also seems to have a role in security behaviour intentions. This suggests that building self-efficacy is important, if teaching pursues behavioural change. Knowledge, skills, cybersecurity and skills specific self-efficacy, and recalled security actions had statistically significantly higher values after teaching than before it. However, pre- and post-measurements do not show statistically significant change in all variables associating with teaching, for example in interest related variables. This implicates that in teaching, we should consider how the interventions are supposed to raise student interest, as interest is connected to motivation and academic success.**

***Keywords*—cybersecurity teaching, effectiveness, self-efficacy, attitude, behaviour, motivation**

I. Introduction

Information systems and their security have a central role in modern society and the need for cybersecurity expertise is high. However, though education is a basis of cybersecurity awareness, culture, and skills [1–9], there is a shortage of experts and deficiencies in computer science curricula [10–13]. Experts should be capable of effectively responding to changing cyberthreats, and security teaching in universities should provide them with necessary awareness, skills, and confidence to do that. This is especially important for software and system developers and organizations that create and maintain information systems for society.

As education and knowledge are the basis of effective security throughout society, it matters how cybersecurity is taught. Teaching should have many outcomes beyond students' cybersecurity knowledge base. Teaching should pass on graduate attributes, such as broad professional and attitudinal dispositions along with knowledge, and maybe even enable *powerful knowledge*, which "equips those who have it with the necessary skills for producing knowledge and evaluating knowledge claims, and to do so within different knowledge contexts" [14, p. 368]. When applied to cybersecurity teaching, powerful knowledge could mean that graduates have the necessary knowledge and skills, awareness and adversarial thinking, and also the ability to apply their knowledge effectively in changing and evolving situations. As experts, they should be able to root good cybersecurity practices into various kinds of organizations, which have their own operating environments, as well as their own established norms, rules, and practices. To reach such goals, teaching should boost students' confidence and enable personal growth towards expertise.

How are the numerous goals achieved in cybersecurity teaching? Previously, the outcomes and effectiveness of university cybersecurity teaching have been measured in various ways. For example, the effectiveness of a cybersecurity course was measured by dropout rate, failure rate, and student learning gain [15]. On the other hand, the effectiveness of learning with a Capture the Flag (CTF) challenge has been measured by self-confidence, enjoyment, and skill and knowledge increase [16]. The effectiveness of a cybersecurity serious game has been measured by analysing the player's interaction data and utilizing a survey study to understand the user experience [17]. Measurements have been made, e.g., of students' interests and self-efficacy towards cybersecurity [18] and of self-esteem, general self-efficacy, perceived efficacy in cybersecurity-related tasks, and career-related variables [19]. Summarizing, different measurements have been used for examining the effectiveness of teaching and learning. However, to the best of our knowledge, there is no research measuring the students' perception of effects of cybersecurity teaching, where the effects cover knowledge and skill gain, cybersecurity attitudes, self-efficacy, and security behaviour before and after being exposed to teaching. What is especially lacking in earlier research, is the part of if and how teaching contributes to these effects.

Manuscript received October 20, 2023; revised December 4, 2023; accepted February 18, 2024, published July 22, 2024.

In this research, we measure the outcomes and effectiveness of cybersecurity teaching. We define that effectiveness in teaching means positive changes in students' posture in any of the following: Knowledge, skills, self-efficacy, attitude and behaviour, interest toward topics, further studies or a career – all in relation to cybersecurity. Based on this definition, we present and test hypotheses of a model that allows us to measure the effects of cybersecurity teaching. The model is created based on relevant literature. We also present the effectiveness assessment in five real cybersecurity teaching interventions.

The model can help other teachers in conducting suitable measurements with the purpose of adjusting their teaching content or methods, if it turns out, for example, that students' self-efficacy or interest decreases after teaching. Our current, and any future measurements increase knowledge regarding relations between various parts of the model, which also include teaching methods, learning materials, and students' motivation in addition to factors that define effectiveness.

This study is organized as follows: Section II establishes the theoretical basis for the model, Section III presents 46 hypotheses derived from the model, Section IV describes the variables needed for testing the hypotheses, Section V presents the tests, Section VI presents effectiveness assessment in a pre-post intervention setup, Section VII discusses the results, and Section VIII presents conclusions and future work.

II. Literatiúre Review and Theory

Security awareness is a key for better defence against cyber threats, in both individual and organisational level [1, 2, 5–8]. To assess security awareness, Kruger and Kearney [3] used the Knowledge-Attitude-Behaviour (KAB) model. The KAB-model is an awareness assessing tool, which has been applied to information and cybersecurity awareness research [20, 21].

The KAB-model suggests that knowledge influences attitude, and attitude controls behaviour. However, subsequent research has argued that the KAB-model cannot alone explain behavioural change. For example, Khan [20] combines KAB with the Theory of Reasoned Action (TRA) and with the Theory of Planned Behaviour (TPB) [22]. Khan adds steps of normative belief towards information security, and intention for information security to the KAB-model [20]. Similar elements are also present in another TBP-based model [6].

Thus, reasons leading to actual behaviour are more complex than mere knowledge and attitude, and in explaining behaviour, beliefs are also important [22]. Beliefs are perceived social pressure to comply with assumed expected behaviour and they are caused by important peers, such as executives and colleagues in an organizational context [6]. Therefore, what people think their important peers are expecting of them can affect behavioural intentions, e.g., a student's security behaviour intentions might be affected if the student thinks that their peers never use the same password in two different accounts.

Behaviour has also been researched in the learning context. Social learning theory [23] examines how environmental and cognitive factors affect learning and behaviour. Observation of other people's behaviour, attitudes, and reactions are important for learning. In addition, attitude has a role in behaviour and learning, but it is still an open question how much attitudes and behavioural intentions explain the actual behaviour of a person. In the security context, attitude towards security affects the use and adoption of security tools and practices recommended by experts [24].

In security trainings in organizations, the goal is to change participants' behaviour towards more secure. Similarly, in cybersecurity teaching in universities, this may be one of the goals. Even more important is how teaching impacts students' motivation and interests. In a learning context, the role of self-efficacy, a belief and confidence of "I can learn this", is significant. Self-efficacy of cybersecurity skills is important for students' interest and also for pursuing a cybersecurity career [19]. In addition, students' confidence in their own abilities is important for students' motivation, and teaching should be conducted in such a manner that it enhances students' belief in their own abilities [25].

Self-efficacy is a concept from social cognitive theory [26] and self-efficacy theory [27]. It is defined as "beliefs in one's capabilities to mobilize the motivation, cognitive resources, and courses of action needed to meet given situational demands" [28, p. 408]. Self-efficacy also has a role in human behaviour. In the security context, this role has been researched, for example, in Refs. [6, 29], where higher self-efficacy was related to higher security behaviour intentions. In contrast to these findings, however, in Ref. [30], instead of changing their behaviour towards more secure, young people with high security self-efficacy tended to use more security software to ensure their security. This shows that there is variation in earlier research regarding how self-efficacy affects behaviour intentions. Further, self-efficacy is related to academic success, as various studies have shown that students with higher self-efficacy trust their own abilities and are self-regulated [29, 31]. General self-efficacy can also maintain motivation, even when task demands are complex and the environment changes rapidly [32].

Motivation towards a subject is important for successful learning [23, 25–27, 31]. For learning, also interest is a key component, and educators should try to develop students' interest to enhance academic performance and motivation [33]. The dependencies between motivation, interest and attitude have been researched, and interest has been found to increase positive attitude and engagement in learning [34]. For motivation, it is important that students consider teaching methods and materials meaningful for their learning. Student satisfaction with the content and materials is also important.

To lay a foundation for our model, we summarised all the components of security awareness and how knowledge, attitude, beliefs, self-efficacy and behaviour are connected. The visual summary of the components is

presented in Fig. 1, which shows the literature-based model and its main components. Here, the awareness consists of the KAB-model, which has been complemented by adding self-efficacy, interest, and normative beliefs and their literature-based associations to other components. In addition, the model shows how literature associates teaching to other components.

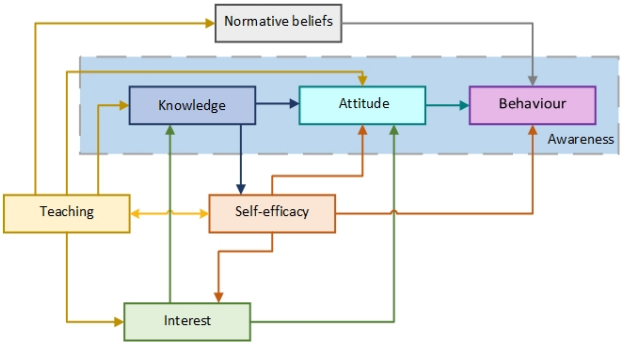

Fig. 1. Literature-based model.

III. Hypotheses

To measure cybersecurity teaching effectiveness, we divided several components of the literature-based model into sub-components, each representing different variables. The resulting detailed model is presented in Fig. 2. The relations among the components of this model are expressed as hypotheses. They are shown together with their test results in Table II. Reasoning that led us to the hypotheses is given below in subsections A–G, which correspond to the 7 main components of the model.

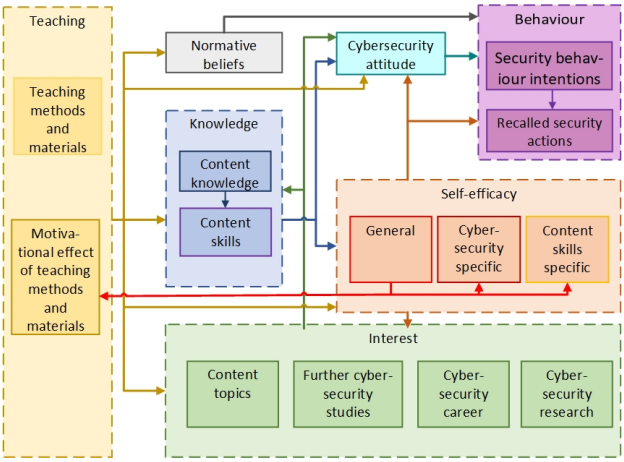

Fig. 2. Detailed model for teaching effectiveness measurement.

A. Teaching

1) Methods and materials (satisfaction and meaningfulness for learning)

Cybersecurity teaching can use many methods, such as lectures, literature, exercises, laboratory exercises, CTFs, and group discussions. Methods and materials influence students' learning, and thus, students' knowledge and skills. Methods can also influence normative beliefs, e.g., students discussing their security practices can influence their conception about expected security behaviour for cybersecurity students. Teaching methods and materials can also influence students' cybersecurity self-efficacy and self-efficacy of content related skills. Thus, we propose the hypotheses H1: a…d. (See Table II.)

2) Motivational effect of teaching methods and materials (attention, relevance, confidence, satisfaction)

Teaching methods and materials can have different motivational effects on students' learning [25] and impact students' knowledge and skills. In the field of mathematics, it has been observed that attitude, academic motivation, and academic achievement have a dependency [35]. We assume that similar dependency is also true for cybersecurity. Teaching may also influence students' cybersecurity self-efficacy, and, further, content skills related self-efficacy. The motivational effect may possibly maintain interest towards content topics, or the other way round, topic interest can support motivation. We hypothesize that the motivational effect can also raise interest in further studies, cybersecurity career, or cybersecurity research. Thus, we propose the hypotheses H2: a…i.

B. Normative Beliefs

As discussed in Section II, according to Ref. [6], normative beliefs are perceived social pressure to behave as expected. Further, the perceived pressure is caused by the important peers. Thus, what people think their important peers are expecting of them is a factor affecting behavioural intentions. This leads us to propose the hypothesis H3.

C. Content Knowledge and Skills Differentiated

1) Knowledge

In the field of cybersecurity skills are an essential part of knowledge and knowledge is essential for skill building. According to the KAB-model [3], knowledge also affects attitude. Knowledge is the basis for all learning that affects learner's self-efficacy regarding the learning topic. Thus, we propose the hypotheses H4: a…d.

2) Skills

Cybersecurity knowledge and skills are intertwined. However, skills do not necessarily grow if teaching does not include activities to train them. For this reason, it is important to measure knowledge and skills separately, as lack of skill building activities in teaching may influence students' self-efficacy. Thus, we propose the hypotheses H5: a…c.

D. Self-Efficacy

1) General

General self-efficacy reflects people's belief in their abilities to cope with different situations, and persons with high general self-efficacy believe they can successfully perform different kinds of tasks [32]. According to Ref. [32] and references therein, general self-efficacy also supports specific self-efficacy in such a way that specific self-efficacy is an outcome of general self-efficacy. Self-efficacy also has a role in behaviour and higher self-efficacy has been related to higher security behaviour intentions [6, 29]. Thus, we propose the hypotheses H6: a…d.

2) Cybersecurity specific

According to Ref. [24], cybersecurity attitude has a correlation with self-efficacy. Further, as self-efficacy and motivation have a relationship, cybersecurity specific self-efficacy may also affect interests towards intervention content, further cybersecurity studies, or a cybersecurity career. For example, Wee, Bashir and Memon [19] report that self-efficacy of cybersecurity skills is important for students' interest and also for pursuing a cybersecurity career. Self-efficacy has also been related to higher security behaviour intentions [6, 29]. There are also studies which have found positive correlation between self-efficacy and attitude toward learning with technology [36, 37]. Thus, we propose the hypotheses H7: a…f.

3) Content skills specific

Content skill specific self-efficacy measures self-efficacy, which is directly related to skills the intervention is supposed to teach. It is important for effective teaching that students' self-efficacy regarding the taught skills raises. Based on the same reasoning as in point D.2 above, we propose the hypotheses H8: a…f.

E. Cybersecurity Attitude

As discussed in Section II, attitude affects behaviour intentions. Thus, we propose the hypothesis H9: a, b.

F. Behaviour

1) Security behaviour intentions

Faklaris, Dabbis, and Hong [24] suggest that security behaviour intentions partially mediate how attitude influences the Recalled security actions. This is consistent with the theory of reasoned action where attitudes and subjective norms affect behavioural intentions leading to actions. Thus, we propose the hypothesis H10.

G. Interest

1) Content topics

As discussed in Section II, interest has dependencies with learning and attitude. As interest has a connection with motivation and interest affects learning behaviour, we also hypothesize that it can affect behaviour in general, and thus also security behaviour intentions. Thus, we propose the hypotheses: H11: a…d.

IV. Variables

We used a survey to evaluate the model. Survey scales and items for measurements were adapted from previous research (see subsections A–G below) for the following variables: Motivational effect of teaching methods and materials, Normative beliefs, General self-efficacy, Cybersecurity specific self-efficacy, Cybersecurity attitude, Security behaviour intentions, and Recalled security actions. In addition, survey items were constructed for the following variables based on the topics and content of each teaching intervention: Methods and materials, Content knowledge and skills, Content skills specific self-efficacy, and Content topics interest. The rest of the interest variables: Further cybersecurity studies, Cybersecurity career and Cybersecurity research were measured with seven separate questions related to career and further interest in studying cybersecurity.

A. Teaching

1) Methods and Materials (sMM)

The survey items are based on the teaching methods and materials, and students assess how meaningful these were for their learning, and how satisfied they felt.

2) Motivational effect of teaching Methods and Materials (sIMM)

For measuring the motivational effect of teaching methods and materials, Attention, Relevance, Confidence, Satisfaction (ARCS) model [25] gives us the 12-item Reduced Instructional Materials Motivation Survey (RIMMS) validated by Loorbach *et al.* [38]. We modified the RIMMS items to fit the teaching materials by changing some of the wording. The RIMMS scale is used in the post-survey because it is tied to teaching experience and students cannot answer it before participating in the teaching.

B. Normative Beliefs (sNB)

We adapted the measurement scale for normative beliefs from Bulgurcu, Gavusoglu, and Benbasat [6], who adapted it from Ajzen [22]. The scale has four items. We considered that important peers for normative beliefs are other students, teachers, colleagues, and authorities.

C. Content Knowledge and Skills

1) Content Knowledge (sCK)

Students' pre-teaching content knowledge was measured by asking students to assess their knowledge of several cybersecurity topics related to the content of teaching. In the post-teaching survey, students assessed the same items again, so that the difference could be measured.

2) Content Skills (sCKS)

Students' pre-teaching content skills were measured by asking students to assess their skills of several cybersecurity topics related to the content of teaching. In the post-teaching survey, students assessed the same items again, so that the difference could be measured.

D. Self-Efficacy

1) General (sGSE)

We measured general self-efficacy with well-researched, validated and reliability-tested New General Self-Efficacy Scale (NGSE) [32].

2) Cybersecurity Specific (sCSE)

We measured cybersecurity specific self-efficacy with the scale developed and tested by Wee, Bashir and Memon [19]. They measured self-efficacy with various scales to study whether overall self-esteem, generalized self-efficacy, and cybersecurity specific self-efficacy affected participants' cybersecurity career intentions after participating in a cybersecurity contest.

3) Content Skills Specific (sCsSE)

We measured content skills specific self-efficacy with items that are the same as the items measuring teaching related skills. This allows us to examine teaching specific

self-efficacy changes and see if the teaching has improved students' self-efficacy related to the taught skills.

E. Cybersecurity Attitude (sATT)

The measurement scale for attitude was SA-6 [24], which has been validated and reliability tested. SA-6 scale is consistent with long-term research evidence showing that attitude and behavioural intention are correlated, and SA-6 also has correlations with other constructs from the theory of planned behaviour, such as self-efficacy and subjective norms [24]. SA-6 is also significantly associated with security behaviour intentions (SeBIS, developed by Egelman and Peer [39]).

F. Behaviour

1) Security Behaviour Intentions (sSIB)

Behavioural intentions were assessed by using Security Behaviour Intentions Scale (SeBIS) [39], which is a 16-item reliability-tested and validated scale for measuring security behaviour intentions. The scale's predictive properties have also been tested by predicting intentions with the scale and then observing participants' actual behaviour in certain situations [40].

2) Recalled Security Actions (sRSA)

Recalled Security Actions inventory (RSec) was used to measure whether participants recalled performing certain security actions during the last week [24]. It is significantly associated with SA-6 security attitude scale [24].

G. Interest

(1) Content topics (sCI)
(2) Further cybersecurity studies (sFSI)
(3) Cybersecurity career (sCarI)
(4) Cybersecurity research (sResI)

Students' cybersecurity interest was divided into four parts: content topics, further studies, career and research. Content topics interest measures cybersecurity interest which is bounded by teaching topics and content. Thus, it cannot be generalized to overall cybersecurity interest. The last three were measured out of curiosity to see whether teaching has any effect on students' future plans related to cybersecurity. Survey items for content topics came from the intervention content. Career, research, and further study interests were measured with seven items, which overlap so that each sub-scale contains three items. This scale is self-developed.

V. Testing the Model Hypotheses

A. Method

We constructed the survey for five different cybersecurity Teaching Interventions (TI) in Tampere University, Finland. Three of them were cybersecurity courses and the rest were CTF exercises. All TIs have a different student profile: TI1 is an advanced cybersecurity course, TI2 is an online cybersecurity basic course mandatory for ITC-students, TI3 is an online basic introduction to cybersecurity for all students regardless of study field, TI4 is a beginner level CTF, and TI5 is an advanced level CTF.

For TIs 1, 2, and 3, students filled the pre-survey before starting the course and post-survey after completing the course. For TIs 4 and 5, students filled the pre-survey before the CTF exercise. The post-survey for CTFs was divided into two parts. The first post-survey was filled right after finishing the CTF exercise and the second post-survey after two weeks. In the second post-survey, we measured behavioural changes (sSBI and sSRA), which could not be asked right after playing. Participation in all the surveys was voluntary. For the hypothesis testing, post-survey data were used. Post-survey participants (N = 177) are presented in Table I.

TABLE I. Participants

Background data		Tot	TI1	TI2	TI3	TI4	TI5
	N	177	20	45	39	47	26
	Males	106	14	29	17	29	17
	Females	70	6	16	21	18	9
	Other	1			1		
Age	under 20	5		1	3	1	
	20-29	122	18	29	20	33	22
	30-39	27	1	9	6	8	3
	40-49	13	1	2	5	4	1
	50-59	7		4	2	1	
	over 60	3			3		
Major	Information security	37	12	2	1	6	16
	ICT	75	6	26	10	25	8
	Engineering	18	1	8	3	6	
	Other	47	1	9	25	10	2
Previous education	Primary school	1				1	
	Upper secondary school	73	6	20	17	21	9
	Vocational education	13		6	6	1	
	Bachelor's degree	70	13	13	11	17	16
	Master's degree	20	1	6	5	7	1

The surveys had several common scales for all five TIs, measured with the same sum variables: sIMM, sNB, sGSE, sCSE, sATT, sFSI, sCarI, sResI, sSBI, and sRSA. For each intervention we tailored the scales for sMM, sCK, sCKS, sCsSE, and sCI, so that they matched the intervention content.

All measurements were self-reported and measured students' own experiences. For Content knowledge and skills, students assessed their knowledge (sCK) and skills (sCKS) of several TI-related cybersecurity topics. Response options for sCK and sCKS were from 1 *I don't know anything about this* to 5 *I know this thoroughly*. Students assessed similarly their Content Interest (sCI) and further studies and career related interests. Response options for sCI, sFSI, sCarI, and sResI were from 1 *I'm not at all interested* to 5 *I'm extremely interested*. Students also assessed their confidence in performing several Cybersecurity tasks (sCSE) and TI content skill related Cybersecurity tasks (sCsSE). Response options for sCSE and sCsSE were from 1 *No confidence at all* to 5 *Completely confident*. Methods and Materials (sMM) scale measured students' experience of satisfaction and meaningfulness of learning about several items related to TI content and teaching. Response options for sMM was from 1 *Not at all* to 5 *Extremely*. The scales sGSE, sNB, sATT, and sIMM measured how much students agree with each item, or how true the item was for students.

Response options for the first three were from 1 *strongly disagree* to 5 *strongly agree*, and for sIMM from 1 *Not true* to 5 *Very true*. In behaviour related scales, students responded how often they perform certain security actions and whether they remember having done certain actions during last week. Response options for sSIB were from 1 *Never* to 5 *Always*, and for sRSA from 1 *No* or *Not sure* to 2 *Yes*.

We examined the reliability of the scales with Cronbach's alpha. All results were above the threshold of 0.7, expect sRSA which was 0.533. Spearman correlation was used for hypotheses testing, as some variables were not normally distributed. All statistics was conducted using IBM SPSS Statistics version 28.0.1.0 (142).

B. Results

The number of responses was lower (N = 141) for variables sSBI and sRSA due to TIs 4 and 5, where behavioural changes were not immediately surveyed after the CTF exercise. Unfortunately, attendance in the latter part of the post-survey was lower than in the preceding post-survey right after the CTF exercise.

TABLE II. THE MODEL HYPOTHESES. SUPPORTED HYPOTHESES ARE HIGHLIGHTED WITH GREEN.

There is a positive relationship between Variable…	**Correlation coefficient**	***p***	**Effect size**	**Supported?**
Teaching methods and materials and				
H1a: Content knowledge.	0.36	< 0.001	moderate	Yes
H1b: Content skills.	0.31	< 0.001	moderate	Yes
H1c: Normative beliefs.	0.14	0.079	weak	No
H1d: Cybersecurity specific self-efficacy.	0.23	0.002	weak	No
H1e: Content skills specific self-efficacy.	0.27	< 0.001	weak	Yes
H1f: Content topic interest.	0.35	< 0.001	moderate	Yes
Motivational effect of teaching methods and materials and				
H2a: Content knowledge.	0.29	< 0.001	weak	Yes
H2b: Content skills.	0.22	0.005	weak	No
H2c: Cybersecurity attitude.	0.25	0.001	weak	Yes
H2d: Cybersecurity specific self-efficacy.	0.17	0.035	weak	No
H2e: Content skills specific self-efficacy.	0.10	0.195	weak	No
H2f: Content topic interest.	0.43	< 0.001	moderate	Yes
H2g: Further cybersecurity studies interest.	0.53	< 0.001	relatively strong	Yes
H2h: Cybersecurity career interest.	0.40	< 0.001	moderate	Yes
H2i: Cybersecurity research interest.	0.29	< 0.001	weak	Yes
H3: Normative beliefs *and Security behaviour intentions.*	0.05	0.566	very weak	No
Content knowledge and				
H4a: Content skills.	0.72	< 0.001	strong	Yes
H4b: Cybersecurity attitude.	0.28	< 0.001	weak	Yes
H4c: Cybersecurity specific self-efficacy.	0.52	< 0.001	relatively strong	Yes
H4d: Content skills specific self-efficacy.	0.58	< 0.001	relatively strong	Yes
Content skills and				
H5a: Cybersecurity attitude.	0.21	0.007	weak	No
H5b: Cybersecurity specific self-efficacy.	0.37	< 0.001	moderate	Yes
H5c: Content skills specific self-efficacy.	0.70	< 0.001	strong	Yes
General self-efficacy and				
H6a: Motivational effect of teaching methods and materials.	0.30	< 0.001	moderate	Yes
H6b: Security behaviour intentions.	0.31	< 0.001	moderate	Yes
H6c: Cybersecurity specific self-efficacy.	0.13	0.095	weak	No
H6d: Content skills specific self-efficacy.	0.20	0.010	weak	No
Cybersecurity specific self-efficacy and				
H7a: Cybersecurity attitude.	0.36	< 0.001	moderate	Yes
H7b: Security behaviour intentions.	0.27	0.001	weak	Yes
H7c: Content interest.	0.38	< 0.001	moderate	Yes
H7d: Further cybersecurity studies interest.	0.31	< 0.001	moderate	Yes
H7e: Cybersecurity career interest.	0.43	< 0.001	moderate	Yes
H7f: Cybersecurity research interest.	0.38	< 0.001	moderate	Yes
Content skills specific self-efficacy and				
H8a: Cybersecurity attitude.	0.17	0.025	weak	No
H8b: Security behaviour intentions.	0.35	< 0.001	moderate	Yes
H8c: Content interest.	0.37	< 0.001	moderate	Yes
H8d: Further cybersecurity studies interest.	0.03	0.726	very weak	No
H8e: Cybersecurity career interest.	0.01	0.908	very weak	No
H8f: Cybersecurity research interest.	0.01	0.865	very weak	No
Cybersecurity attitude and				
H9a: Security behaviour intentions.	0.50	< 0.001	relatively strong	Yes
H9b: Recalled security actions.	0.34	< 0.001	moderate	Yes
H10: Security behaviour intentions *and Recalled security actions.*	0.40	< 0.001	moderate	Yes
Content topic interest and				
H11a: Content knowledge.	0.53	< 0.001	relatively strong	Yes
H11b: Content skills.	0.42	< 0.001	moderate	Yes
H11c: Cybersecurity attitude.	0.39	< 0.001	moderate	Yes
H11d: Security behaviour intentions.	0.31	< 0.001	moderate	Yes

To test the hypotheses, we calculated two-tailed Spearman correlations between variables. As we were testing multiple hypotheses (46), we used Bonferoni correction and expected that the alpha level is at least 0.05/46 = 0.0011. Thus, we only accepted $p \leq 0.001$ correlations as statistically significant.

Table II presents hypotheses, correlation coefficients, p-values, effect sizes, and whether the hypothesis is statistically supported or not. According to the results, hypotheses H1: a, b, e, f; H2: a, c, f...i; H4: a...d; H5: b, c; H6: a, b; H7: a...f; H8: b, c; H9: a, b; H10, H11: a...d were supported, and the rest were not. All supported hypotheses are visualized in Fig. 3.

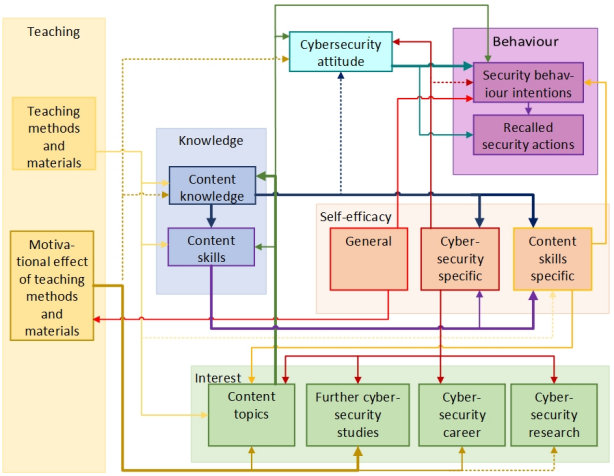

Fig. 3. Supported model hypotheses. Thickest arrows: Relatively strong or strong correlations, dashed arrows: Weak correlations. Rest of the arrows present moderate correlations.

VI. Effectiveness Assessment in Pre-post Intervention Setup

A. Method

To measure the effectiveness of the TIs, we compared variables in pre- and post-surveys among the same students. We expected the students would report different values of variables after attending a TI. We also expected the students who participated in the TI would report different values of variables than students who did not participate. Overall, we expected that participation in the TI would raise the variable values. All hypotheses and results of their tests are presented in Table III.

For the pre-post-tests, we used paired data from the pre- and post-surveys. Only students who had taken both the pre- and post -surveys, were selected. The total number of pairs was 88. The number of pairs was lower for variables sSBI and sRSA, due to lower attendance of the second post survey in TIs 4 and 5 (N = 64). We also compared unlinked pre-survey responses to post-survey responses to see if the changes matched with pre-post group responses. The pre-group consists of students, who had responded to the pre-survey, but had not taken the post-survey. The number of unlinked pre-survey responses was 209.

To test the pre-post hypothesis, we used the Wilcoxon signed rank test for paired sample (pre-post group) and the Mann-Whitney U-test for the independent sample (pre-group vs. post-group), as the measured data was not normally distributed. All statistics were conducted using IBM SPSS Statistics version 28.0.1.0 (142).

B. Results

As we were testing multiple hypotheses (2), we used Bonferoni correction and expected that the alpha level is at least 0.05/2 = 0.025. Thus, we only accepted $p < 0.025$ as statistically significant.

There is a statistically significant difference in both paired sample and independent sample tests in Content Knowledge (sCK), Content Skills (sCKS), Cybersecurity Specific Self-Efficacy (sCSE), Content Skills Specific Self-Efficacy (sCsSE), and Recalled Security Actions (sRSA). In all these, the difference is positive, i.e., post-values are higher than pre-values. For variables Career Interest (sCarI) and Research Interest (sResI), the difference is negative but not significant. All the remaining variables show a positive but non-significant difference. Thus, we found support for hypotheses H12: a…c, H13: a…c, H15: a…c, H16: a…c, H22: a…c, and not for the rest.

TABLE III. Paired Sample (A) and Independent Sample (B) Test Results. Supported Hypotheses Are Highlighted with Green.

Variable	z	p	Effect size	Supported?
Content knowledge				
H12a:	−7.146	< 0.001	0.77	Yes
H12b:	−8.45	< 0.001	0.44	Yes
Content skills				
H13a:	−6.785	< 0.001	0.73	Yes
H13b:	−4.122	< 0.001	0.21	Yes
Cybersecurity attitude				
H14a:	−0.960	0.337	0.10	No
H14b:	−1.333	0.183	0.07	No
Cybersecurity specific self-efficacy				
H15a:	−2.774	0.006	0.30	Yes
H15b:	−2.626	0.009	0.14	Yes
Content skills specific self-efficacy				
H16a:	−5.018	< 0.001	0.54	Yes
H16b:	−2.594	0.009	0.13	Yes
Content interest				
H17a:	−0.483	0.629	0.05	No
H17b:	−0.251	0.802	0.01	No
Further study interest				
H18a:	−0.276	0.782	0.03	No
H18b:	−0.861	0.389	0.04	No
Career interest				
H19a:	−0.525	0.600	0.06	No
H19b:	−0.079	0.937	0.00	No
Research interest				
H20a:	−0.339	0.735	0.04	No
H20b:	−0.402	0.688	0.02	No
Security behaviour intentions				
H21a:	−0.728	0.467	0.09	No
H21b:	−1.160	0.246	0.06	No
Recalled security actions				
H22a:	−2.653	0.008	0.33	Yes
H22b:	−3.230	0.001	0.17	Yes

Note: Variable (X = 12, …, 22)
*HXa: Post-**survey** Variable significantly differs from pre-**survey** Variable. (A)*
*HXb: Post-**group** Variable significantly differs from pre-**group** Variable. (B)*

VII. Discussion

We first return to interpreting the results from Section V, related to our model. We found moderate to strong positive correlations between teaching variables and Content knowledge, Content skills, Content topic interest, Further cybersecurity studies interest and Cybersecurity career interest. Teaching methods and materials have a moderate relationship with Content knowledge, Content skills, and Content topic interest. Thus, students who assess their knowledge, skills, and interest higher are more satisfied with methods and materials. Teaching methods and materials also have a weak correlation with Content skills specific self-efficacy, thus students rating teaching methods and materials higher also have higher values in Content specific self-efficacy.

However, Teaching methods and materials do not show a relationship with Further interest in cybersecurity studies, nor Cybersecurity career interest or Cybersecurity research interest. Instead, these associations are visible via the Motivational effect of teaching methods and materials, as students with higher values in motivational effect rate their interest higher in Content topics, Further cybersecurity studies, Cybersecurity career, and Cybersecurity research. The relationship is relatively strong with Further studies interest and moderate with the rest. In addition, students with higher values in motivational effect have higher values in Content knowledge and Cybersecurity attitude, although these relationships are weak. Thus, these results also suggest that motivation, interest, and attitude have a relationship as observed in earlier research [33, 34].

TI Content knowledge and skills have a strong correlation with both cybersecurity related self-efficacy variables indicating that students who assess their knowledge and skills higher, also assess self-efficacy related variables higher. Students with high General self-efficacy also rate the Motivational effect of teaching methods and materials and Security behaviour intentions higher. Thus, students with high general self-efficacy find the intervention teaching more motivating. The result is in line with earlier research results of self-efficacy having a relationship with academic success [29, 31].

Cybersecurity specific self-efficacy moderately correlates with interests in Content topics, Further cybersecurity studies, and Cybersecurity career and research. Also, Content skills specific self-efficacy has a relationship with Content topic interest. Thus, students with higher Cybersecurity specific self-efficacy also have higher interest towards Content topics, Further cybersecurity studies, Cybersecurity career, and Cybersecurity research. The result is in line with those in [19], where it is shown that self-efficacy of cybersecurity skills is important for students' interest in cybersecurity and also for pursuing cybersecurity career.

All self-efficacy variables also have a correlation with Security behaviour intentions, and effect sizes are moderate for General and Content skills specific self-efficacy and weak for Cybersecurity specific self-efficacy. Thus, students with higher self-efficacy have higher intentions for secure behaviour. This suggests that building self-efficacy is important when the intervention pursues behavioural change. However, self-efficacy is not directly influencing Recalled security actions. Instead, higher Cybersecurity attitudes and higher Security behaviour intentions have a relationship with higher Recalled security actions. Self-efficacy seems to have a mediating role when actual security actions are considered.

A contradicting result with earlier research is that in our measurements, Normative beliefs did not have any role in behaviour intentions, unlike in Ref. [6]. Instead, our result suggests that self-efficacy related variables are more important than normative beliefs for behaviour intentions. The difference might be due to a different measurement context, as Bulgurcu, Cavusoglu, and Benbasat [6] studied employees in different US organizations, but we studied Finnish university students. Maybe in a learning context the importance of self-efficacy is emphasized and its effect to behaviour intentions is stronger than the effect of normative beliefs, which could be more important for people in work life, where they must comply with organizational norms.

Despite finding relationships between teaching and some of the variables, we cannot say anything about the causality between variable relationships. Due to voluntary participation, self-selection bias may have affected the results, though participants were offered course points as rewards for participating.

Now, let us discuss results from Section VI. When differences between pre- and post-teaching are examined, we found that Content knowledge, Content skills, Cybersecurity specific self-efficacy, Content skills specific self-efficacy, and Recalled security actions had higher post- than pre-values in the pre-post group. The effect sizes in Content knowledge, Content skills, and Content skills specific self-efficacy were medium. Thus, it seems that participation in teaching has increased values of these variables. However, since we did not have a control group in the TI measurements, we cannot say for sure that these increases are only due to teaching.

It is also interesting that in the pre-post-tests, there is no statistically significant change in all variables, which is associated with teaching in Table III. For example, there is no statistically significant change in any of the interest variables in the pre- and post-groups. This may indicate that teaching, at least in this form, does not have a significant impact on student interests. Instead, interest may be something that students already have or don't have when they come to a class, and teaching does not change this pre-position significantly. Interest, however, is correlated with several variables which we hope to increase with our teaching, and in terms of effectiveness, it would be very important to be able to raise students' interest. Maybe it is also a matter of how we teach, implicating that more attention should be given in making the intervention content interesting for students.

VIII. Conclusion and Future Work

In this study, we developed a model to evaluate the effectiveness of cybersecurity education. In five teaching

interventions, we measured students' knowledge, skills, interests, attitudes, self-efficacy, behavioural intentions, and motivational factors related to teaching material and methods. Their statistical interdependencies, including those that show changes from pre-intervention to post-intervention, suggest the potential utility of our model.

In particular, we found teaching has moderate to strong positive correlations with knowledge, and skills, as well as topic, further study and career interests. Knowledge and skills have a strong correlation with both cybersecurity related self-efficacy variables. Results also indicate that students with higher cybersecurity specific self-efficacy have a higher interest towards intervention topics, further cybersecurity studies, cybersecurity career, and cybersecurity research. Self-efficacy also seems to have a role in security behaviour intentions. This suggests that building self-efficacy is important, when the intervention pursues behavioural change.

Recall the practical question: Does our teaching promote a wide set of effectiveness goals? The answer given by the study at this stage is the observation of higher values after teaching than before regarding the following goals: Content knowledge, Content skills, Cybersecurity specific self-efficacy, Content skills specific self-efficacy, and Recalled security actions. However, pre- and post-measurements do not show statistically significant change in all variables associating with teaching, for example in interest related variables. This implicates that in teaching, we should consider how the interventions are supposed to raise student interest, as interest is connected to motivation and academic success. At the next stage, we should also investigate, how much our teaching affects. During such measurements, it would be good to address especially the needs of low-achieving students, because they are likely to benefit most from improved teaching.

In the future, we will also gather more data from different TIs which will allow analysis for individual TIs, while now our treatment combines all five. This will let us compare individual courses and CTF exercises. We also plan to extend the research to different countries. Future research should also enable control groups and reduce self-selection bias if possible.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Surveys were constructed by all authors. TS-T analyzed the data and wrote the paper; JK edited the text; JK and MH provided feedback and suggestions; all authors had approved the final version.

Funding

This research was partly funded by European Research Council (ERC), Grant Agreement number: 804476 — SCARE — ERC-2018-STG.

References

[1] L. Hadlington, "Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom," *Int. J. Cyber Criminol.*, vol. 12, no. 1, pp. 269–281, Oct. 2018. doi: 10.5281/ZENODO.1467909

[2] M. Alshaikh, "Developing cybersecurity culture to influence employee behavior: A practice perspective," *Comput. Secur.*, vol. 98, 102003, Nov. 2020. doi: 10.1016/j.cose.2020.102003

[3] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Comput. Secur.*, vol. 25, no. 4, pp. 289–296, Jun. 2006. doi: 10.1016/j.cose.2006.02.008

[4] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Inf. Manag. Comput. Secur.*, vol. 18, no. 5, pp. 316–327, Nov. 2010. doi: 10.1108/09685221011095236

[5] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: A comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Jan. 2022. doi: 10.1080/08874417.2020.1712269

[6] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, p. 523, 2010. doi: 10.2307/25750690

[7] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. Inf. Manag.*, vol. 45, pp. 13–24, Apr. 2019. doi: 10.1016/j.ijinfomgt.2018.10.017

[8] I. Kirlappos, S. Parkin, and M. A. Sasse, "'Shadow security' as a tool for the learning organization," *ACM SIGCAS Comput. Soc.*, vol. 45, no. 1, pp. 29–37, Feb. 2015. doi: 10.1145/2738210.2738216

[9] E. Kweon, H. Lee, S. Chai, and K. Yoo, "The utility of information security training and education on cybersecurity incidents: An empirical evidence," *Inf. Syst. Front.*, vol. 23, no. 2, pp. 361–373, Apr. 2021. doi: 10.1007/s10796-019-09977-z

[10] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput. Secur.*, vol. 119, 102754, Aug. 2022. doi: 10.1016/j.cose.2022.102754

[11] B. J. Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?" *Educ. Inf. Technol.*, vol. 27, no. 3, pp. 3011–3036, Apr. 2022. doi: 10.1007/s10639-021-10704-y

[12] O. Osunji, "Bridging the disconnect within cybersecurity workforce supply chain," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 9, no. 1, p. 6, Mar. 2022. doi: 10.53735/cisse.v9i1.136

[13] B. Scott and R. Mason, "Cyber as a second language? A challenge to cybersecurity education," *J. Colloq. Inf. Syst. Secur. Educ.*, vol. 9, no. 1, p. 6, Mar. 2022. doi: 10.53735/cisse.v9i1.137

[14] N. Wald and T. Harland, "Graduate attributes frameworks or powerful knowledge?" *J. High. Educ. Policy Manag.*, vol. 41, no. 4, pp. 361–374, Jul. 2019. doi: 10.1080/1360080X.2019.1613310

[15] P. Deshpande, C. B. Lee, and I. Ahmed, "Evaluation of peer instruction for cybersecurity education," in *Proc. the 50th ACM Technical Symposium on Computer Science Education*, Feb. 2019, pp. 720–725. doi: 10.1145/3287324.3287403

[16] K. Leune and S. J. Petrilli, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proc. the 18th Annual Conference on Information Technology Education*, Sep. 2017, pp. 47–52. doi: 10.1145/3125659.3125686

[17] S. Kulshrestha, S. Agrawal, D. Gaurav, M. Chaturvedi, S. Sharma, and R. Bose, "Development and validation of serious games for teaching cybersecurity," in *Serious Games. JCSG 2021. Lecture Notes in Computer Science*, B. Fletcher, M. Ma, S. Göbel, J. B. Hauge, and T. Marsh, Eds., Cham: Springer, 2021, vol. 12945, pp. 247–262. doi: 10.1007/978-3-030-88272-3_18

[18] R. Bell, E. Vasserman, and E. Sayre, "Developing and piloting a quantitative assessment tool for cybersecurity courses," in *Proc. 2015 ASEE Annual Conference and Exposition*, Jun. 2015, pp. 26.496.1–26.496.13. doi: 10.18260/p.23835

[19] J. M. C. Wee, M. Bashir, and N. Memon, "Self-efficacy in cybersecurity tasks and its relationship with cybersecurity competition and work-related outcomes," in *Proc. 2016 USENIX Workshop on Advances in Security Education*, 2016, p. 8.

[20] B. Khan, "Effectiveness of information security awareness methods based on psychological theories," *Afr. J. Bus. Manag.*, vol. 5, no. 26, Oct. 2011. doi: 10.5897/AJBM11.067
[21] A. McCormac, D. Calic, M. Butavicius, K. Parsons, T. Zwaans, and M. Pattinson, "A reliable measure of information security awareness and the identification of bias in responses," *Australas. J. Inf. Syst.*, vol. 21, Nov. 2017. doi: 10.3127/ajis.v21i0.1697
[22] I. Ajzen, "The theory of planned behaviour," *Organ. Behav. Hum. Decis. Process*, vol. 50, pp. 179–211, 1991.
[23] A. Bandura, *Social Learning Theory*, New York: General Learning Press, 1971.
[24] C. Faklaris, L. Dabbish, and J. I. Hong, "A self-report measure of end-user Security Attitudes (SA-6)," in *Proc. the Fifteenth Symposium on Usable Privacy and Security*, 2019, pp. 61–77.
[25] J. M. Keller, *Motivational Design for Learning and Performance*. Boston, MA: Springer US, 2010. doi: 10.1007/978-1-4419-1250-3
[26] A. Bandura, *Social Foundations of Thought and Action: A Social Cognitive Theory*, Englewood Cliffs: Prentice Hall, 1986.
[27] A. Bandura, "Self-Efficacy: Toward a unifying theory of behavioral change," *Psychol. Rev.*, vol. 84, no. 2, 1977.
[28] R. Wood and A. Bandura, "Impact of conceptions of ability on self-regulatory mechanisms and complex decision making," *J. Pers. Soc. Psychol.*, vol. 56, no. 3, pp. 407–415, 1989.
[29] M. Bishop, I. Ngambeki, S. Mian, J. Dai, and P. Nico, "Measuring self-efficacy in secure programming," in *Information Security Education for Cyber Resilience. WISE 2021. IFIP Advances in Information and Communication Technology*, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. von Solms, Eds., Cham: Springer, 2021, vol. 615, pp. 81–92. doi: 10.1007/978-3-030-80865-5_6
[30] B. Xue, M. Warkentin, L. A. Mutchler, and P. Balozian, "Self-Efficacy in information security: A replication study," *J. Comput. Inf. Syst.*, pp. 1–10, Dec. 2021. doi: 10.1080/08874417.2021.2015725
[31] B. J. Zimmerman, "Self-Efficacy: An essential motive to learn," *Contemp. Educ. Psychol.*, vol. 25, no. 1, pp. 82–91, Jan. 2000. doi: 10.1006/ceps.1999.1016
[32] G. Chen, S. M. Gully, and D. Eden, "Validation of a new general self-efficacy scale," *Organ. Res. Methods*, vol. 4, no. 1, pp. 62–83, Jan. 2001. doi: 10.1177/109442810141004
[33] S. Hidi, "Interest: A unique motivational variable," *Educ. Res. Rev.*, vol. 1, no. 2, pp. 69–82, Jan. 2006. doi: 10.1016/j.edurev.2006.09.001
[34] T. Flowerday and D. F. Shell, "Disentangling the effects of interest and choice on learning, engagement, and attitude," *Learn. Individ. Differ.*, vol. 40, pp. 134–140, May 2015. doi: 10.1016/j.lindif.2015.05.003
[35] M. Moenikia and A. Zahed-Babelan, "A study of simple and multiple relations between mathematics attitude, academic motivation and intelligence quotient with mathematics achievement," *Procedia – Soc. Behav. Sci.*, vol. 2, no. 2, pp. 1537–1542, 2010. doi: 10.1016/j.sbspro.2010.03.231
[36] H. K. Yau and Y. F. Leung, "The relationship between self-efficacy and attitudes towards the use of technology in learning in Hong Kong higher education," in *Proc. the International MultiConference of Engineers and Computer Scientists 2018*, 2018, pp. 832–834.
[37] X. Pan, "Technology acceptance, technological self-efficacy, and attitude toward technology-based self-directed learning: learning motivation as a mediator," *Front. Psychol.*, vol. 11, 564294, Oct. 2020. doi: 10.3389/fpsyg.2020.564294
[38] N. Loorbach, O. Peters, J. Karreman, and M. Steehouder, "Validation of the Instructional Materials Motivation Survey (IMMS) in a self-directed instructional setting aimed at working with technology: Validation of the IMMS," *Br. J. Educ. Technol.*, vol. 46, no. 1, pp. 204–218, Jan. 2015. doi: 10.1111/bjet.12138
[39] S. Egelman and E. Peer, "Scaling the security wall: Developing a Security Behavior Intentions Scale (SeBIS)," in *Proc. the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Apr. 2015, pp. 2873–2882. doi: 10.1145/2702123.2702249
[40] S. Egelman, M. Harbach, and E. Peer, "Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS)," in *Proc. the 2016 CHI Conference on Human Factors in Computing Systems*, May 2016, pp. 5257–5261. doi: 10.1145/2858036.2858265