Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 47 months

Cyber Security for Europe

D9.26

Awareness Effectiveness Study 3

Document Identification	
Due date	31 November 2022
Submission date	20 December 2022
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary (NTNU)
Contributing Beneficiaries	NTNU, TDL, ATOS, JAMK, UM	Related Deliverables	D9.13, D9.18

Abstract: This report follows from D9.18—Awareness Effectiveness Study 2, in which we conducted a literature review to elicit a comprehensive list of factors relevant to enhancing the effectiveness of cybersecurity awareness, specifically motivating people to adopt and improve cybersecurity behaviour. In this report, we have condensed and validated the outcomes of report D9.18. The compiled list of factors that could be used to motivate people to adopt and change cybersecurity is more complete and practically implementable. In order to achieve this, we used the Delphi approach with 22 experts and two rounds of online surveys. The study identified seven factors that could be used to motivate cybersecurity behaviour adoption and modification.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This is the third and last report in the "Awareness effectiveness study" series. The first report D9.13 was a complete study in which we proposed metrics for cybersecurity awareness evaluation, which has now been published in the Journal of Cybersecurity. Its work continues the research study begun in D9.18, with the goal of eliciting factors that could motivate people to acquire good security behaviour and alter their bad security behaviour. In order to elicit factors that potentially motivate cybersecurity behaviour adoption and modification, the D9.18 report conducted a non-systematic literature review of papers from many fields of study. As a result, it succeeded to elicit a long list of factors for the purpose. The major challenges with the obtained list of factors, however, are, first, it has too many factors making them practically infeasible to implement, and second, it may have contained some less significant factors while overlooking some important factors.

In this report, therefore, we used the Delphi method with 22 experts from various fields of study and nationalities comprising both academic and non-academic professionals. The Delphi method was conducted using two rounds of online surveys. Herein, the main objectives were to narrow down the obtained list of factors to only the most significant ones and include the important factors that the literature review may have missed.

In the first round of the online survey, we asked the experts to assess the importance of knowledge and skills from various fields of study for cybersecurity behaviour adoption and change. Interestingly, the majority of experts found all the specified fields of study to be either important or very important for the stated objective. The specified fields of study were:

- Psychology and human behaviour
- Persuasion theory
- Nudge theory
- Cognitive theory
- Framing theory
- Communication theory
- Pedagogic theory

In the second round of the survey, the experts were asked to select only the "must-haves" factors from the above-mentioned fields of study. It yielded 26 factors with more than 60% of the experts citing them as "*must-haves*". We discovered that majority of these factors are related to message framing. Following an analysis of these factors with the goal of grouping related factors, we obtained seven major factors, namely,

- Management support for and participation in cybersecurity activities
- Cybersecurity to be an ongoing process
- Cybersecurity to be a social norm
- Incentives for cybersecurity actions
- Persuasive framing of cybersecurity messages
- Effective communication of cybersecurity messages
- User-friendly presentation of cybersecurity messages

As a result, it is strongly advised to consider the aforementioned aspects in order to motivate cybersecurity behaviour adoption and change.

Document information

Contributors

Name	Partner
Sunil Chaudhary	NTNU
Vasileios Gkioulos	NTNU
Marko Kompara	UM

Reviewers

Name	Partner
David Goodman	TDL
Christine Jamieson	TDL
Stephan Krenn	AIT
Anni Karinsalo	VTT

History

Version	Date	Authors	Comment
0.01	2022-06-01	Sunil Chaudhary	1st Draft
0.02	2022-11-09	Sunil Chaudhary	2nd Draft
0.03	2022-11-23	Sunil Chaudhary	Integrated feedback from the reviewers.
0.04	2022-12-08	Sunil Chaudhary	Integrated feedback from the reviewer.
0.05	2022-12-13	Sunil Chaudhary	Integrated feedback from the reviewer.
1.0	2022-12-20	Ahad Niknia	Final check, preparation and submission process

Table of Contents

List of Figures

List of Tables

List of Acronyms

C	**CSA**	Cybersecurity Awareness
	CSB	Cybersecurity Behaviour
D	**DP**	Descriptive Psychology
E	**EAST**	Easy, Attractive, Social, and Timely
L	**LR**	Literature Review
M	**MINDSPACE**	Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments, and Ego
S	**SETA**	Security Education, Training, and Awareness

1 Introduction

This report is a continuation of the D9.18 report [1] submitted to CyberSec4Europe. The D9.18 report used a non-systematic literature review (LR) to elicit a list of factors that need to be considered in order to motivate people to adopt and change cybersecurity behaviour (CSB). To make the list as comprehensive as possible, the factors have been drawn from several disciplines including behavioural theory, framing theory, communication theory, pedagogical approach, social and behavioural economics (namely persuasion principle, nudge theory, cognitive and cultural biases, and incentives), usable security, and human traits. However, the obtained list contains a long series of factors, which would be impractical to address. Further, all the factors may not be significantly valuable for CSB purposes. As a result, in this report, we consult experts from several disciplines using the Delphi method to identify and validate the factors that are *must-haves* for the purposes. We believe that doing this will assist to reduce the list size and present the most logical and practically implementable aspects. Additionally, the Delphi method, and more specifically the participating experts, will contribute to identifying the factors that are *must-haves* but have been missed out on the list.

2 Concept of cybersecurity behaviour

Before delving into the study's main objective (i.e., factors that must be addressed or utilised, depending on the situation, to motivate CSB adoption and change), we believe that it is important to clarify the concept of *CSB*. When the term is used, it is often assumed that everyone understands what the term meant, and mostly left up to the individual's intuition and interpretation. Moreover, CSB is often studied from the organisational perspective, wherein it is largely viewed in terms of adherence (i.e., a function of compliance or non-compliance) to policies and regulations [2]. Due to this attitude of taking the term to be self-explanatory, in practice, people often understand and use it inconsistently and incorrectly. Also, possibly influenced by the absence of a recognised pragmatic understanding of the term, a variety of techniques (but mainly questionnaire-based self-reported methods) are used to investigate CSB [3], or to be precise, the perspective of intentions rather than truly CSB [1] [4]. For example, during the review process for the report D9.18, we observed that CSB generally has been depicted as:

- compliance with security rules, regulations, policies, and recommendations,
- usage of information systems security measures,
- prevention of cyber security errors,
- adherence to security good practices or hygiene, and
- action to defend networks and systems.

The above-mentioned observable phenomena convey only partial and contextual meaning of CSB. CSB, in reality, incorporates much more in addition to these portrayals of the end results. For example, they have overlooked the cognitive aspects and other intricacies of behaviour. Therefore, our attempt is to analyse the term to deduce a clear interpretation or understanding of it, both for the users and readers of the term, and more importantly one that could serve for scientific research. However, by this, our intention is not to have a canonical definition of the term.

Indeed, some studies have made efforts to interpret the meaning of CSB and provide its taxonomy. For instance, Mashiane & Kritzinger [2] define CSB as "*an individual's actions, reactions, mannerisms, and general conduct in the cyber domain*." They go on to explain that the context, or the circumstances surrounding a behaviour, can influence CSB. Furthermore, the influence could be either interior, such as self-motivation, or exterior, such as the environment. We would argue that while this definition may apply

to online or Internet behaviour, it cannot be accepted as a definition of CSB since it excludes the main point, i.e., the purpose of behaviour. Similarly, Warkentin *et al.* [5] showed that interaction between the environment and the individuals within it leads to CSB. Several factors such as culture, policies, participation in the Security Education, Training and Awareness Programme (SETA), organisational structure, managerial participation, and leadership are environmental influences [4]. Once again, this study states the endeavours that can affect CSB, but it does not define or explain what CSB actually entails.

Next, based on the levels of expertise and intentions of the individuals, Stanton *et al.* [6] classified CSB into six categories, which are *intentional destruction, detrimental misuse, dangerous tinkering, naïve mistakes, aware assurance,* and *basic hygiene*. Similarly, Mashiane & Kritzinger's [2] made up four categories of CSB based on the intention of individuals, which are *intentional bad, unintentional bad, unintentional good,* and *intentional good*. Both taxonomies divulge the different outcomes of online or Internet behaviour, and at the same time also cover the essence of CSB. For example, if the positive outcomes (i.e., aware assurance, basic hygiene, intentional good) are referred to as good CSB, the other can be referred to as poor CSB. However, these taxonomies still do not address the semantic confusion of CSB.

Although these definitions and taxonomies are informative, they concentrated on only the superficial aspects of CSB. They do not serve a pragmatic explanation and understanding of CSB that would be required for its in-depth scientific study. For example, we specify a behaviour (e.g., all employees in the organisation need to have a strong password) and accordingly apply the needful influences. Now suppose, the organisation experiences that the set objective has not been achieved and thus requires further investigation to resolve the issue. With these definitions and taxonomies, there is not much room left to know what needs to be investigated. As a result, we decided to borrow and adapt the concept of behaviour from Descriptive Psychology (DP), which could serve a more comprehensive and pragmatic understanding of CSB for scientific purposes.

The DP asserts behaviour to be an empirical phenomenon that is amenable, not to definition, but to parametric analysis, and thus formulates the empirical domain of behaviour using eight parameters [7]. The DP formulation for behaviour when used for CSB purposes takes the form as follows:

$$< B >=< I, W, K, K-H, P, A, PC, S >$$

Where….

- *B=Behaviour*: CSB (e.g., Harry changes the password of his organisation's email account)
- *I=Identity*: the identity of the individual whose behaviour it is (e.g., Harry)
- *W=Want*: state of affairs that the individual seeks to bring about (e.g., changing the password successfully, keeping the organisation's email information private, complying with the email security policies)
- *K=Know*: the distinction concepts which are made and acted on (e.g., organisation's email account vs. other email accounts, password vs. other authentication mechanisms, change password vs. other operations like login to an email account, strong password vs. weak password)
- *K-H=Know-How*: the skill or competency being employed with intent to achieve the behaviour (e.g., skill to use the Internet and email, skill to change password, skill to create strong password)
- *P=Performance*: the process, or procedural aspects of the behaviour, including all bodily postures, movements, and processes which are involved in the behaviour (e.g., typing keyboard, moving a mouse, thinking of a new strong password)
- *A=Achievement*: the outcome of the behaviour (e.g., having the password changed, having the new password that is strong and memorable, having able to log in by using the new password)
- *PC=Personal Characteristics*: the personal characteristics of which the behaviour in question is an expression (e.g., knowledge of the Internet and email, knowledge of cybersecurity, seriousness about personal and professional security)

- *S=Significance*: the more inclusive patterns of behaviour enacted by virtue of enacting the behaviour in question (e.g., by participating in the digitisation initiatives, by participating in cybersecurity initiatives)

The aforementioned formulation is more pragmatic and suitable for scientific purposes. It includes goals to achieve, preferences to act on, skills to exercise, physical processes to engage in, outcomes to achieve, personal qualities to express, and significant acts to engage in as components of CSB, thus providing a more holistic view of CSB. In principle, two behaviours can be called identical only if the values for these parameters are identical. In practice, however, people make descriptive commitments to only those parameters that assist their purpose in providing a specific description. This notion could be used to evaluate whether the predetermined goal from CSA activities has been achieved or not.

Let us take an example where want (*W*), know-how (*K-H*), and achievement (*A*) parameters could be significant to CSB purposes. If an employee performed a good CSB, such as, not clicking the link in a phishing email (A), and we want to know if this action was a result of phishing awareness campaigns in the organisation and not a one-time fluke, it must be established that the action was motivated by a desire for phishing protection (*W*), and the individual was aware that the email was a phishing attempt (*K-H*).

Similarly, once again if we consider the earlier case (e.g., all employees in the organisation need to have a strong password but the outcome is not per expectation), then the investigation can still continue in the direction of knowing,

- *Is there insufficient motivation for the employee (W)?*
- *Does the employee lack the necessary knowledge and skills (K-H)?*
- *Is the asked behaviour hard to achieve due to the system's poor usability or the employee's physical disabilities (P)?*
- *Is it due to the personality, culture, or other traits of the employee (PC)?*
- *Does the asked behaviour (or cybersecurity) seem to be insignificant for the employee (S)?*

In a nutshell, CSB can be referred to as "*actions (or, occasionally, inactions) from an individual taken at a valid time and in the rational state of mind in order to achieve a definite set of related security objectives*."

3 List of factors for cybersecurity behaviour

The set of factors that can be used to motivate CSB adoption and change as elicited in the deliverable report D9.18 has been listed in Table 1.

Discipline	Recommendation
Behaviour Theory	• Elevate the perceived severity, response efficacy, self-efficacy, subjective norms, perceived benefits of compliance, perceived cost of non-compliance, perceived usefulness, and perceived ease of use. • Lower the response cost, perceived cost of compliance, and perceived severity of sanctions.
Framing Theory	• Select or include only information that needs to be known by the audience. • Use features to make the information more salient (like strategic positioning, repeating, and linking with culturally known symbols). • Address and if possible, utilise the various cognitive biases (e.g., Loss aversion, Confirmation bias, Hyperbolic discounting, Affect heuristic, Cognitive friendly, Bandwagon effect, and Social proof theory) and other techniques (e.g., do not exacerbate cybersecurity, give a face to the hero and villain in the fight of cybersecurity, connect cybersecurity to issues and values

	other than security alone) to improve the clarity, persuasiveness, and memorability of the message. • Personalise the message (based on information like personal and cultural values, learning style, security perception, and personality traits) for the target audience group. • Use a descriptive format for the message presentation, except for the organisational awareness where a prescriptive format could be preferable. • Ensure that the message is complete (state the problem, assess and identify its causes, evaluate causal agents and their effects or impacts, and recommend remedies). • Positively phrase and frame the message. • Use a compelling message with clear calls for doable action. • Place the most important information at the beginning and end of the information series, and • Use simple language for composing the message.
Communication Theory	• Acknowledge the audience's diversity and consider grouping them preferably based on their cybersecurity pre-existing beliefs/ attitudes and security expertise levels so that the message and communication strategies could be targeted to a specific audience group. • Use features like correctness (in language and facts), unbiasedness, politeness (considerate of other people), conciseness (brief, to the point, and comprehensible), clarity (specific goal, simple language), and concreteness (clear with facts and figures, no ambiguity or chance of misinterpretation) in the content. • Ensure completeness in the message (get attention, establish the need, satisfy the need, visualise the future, and action/actualisation). • Use a communicator who is trustworthy, with expertise, and authority. • Utilise vertical communication for the aspects of security that are critical and integral parts of core business operations and horizontal communication for the general concepts or advice on security issues, however, both should be non-technocratic two-way communication (non-technocratic so that everyone finds comfortable to use it and two-way so to receive feedback from the audience. • Use delivery channels that best fit the content, as well as the audience, who should feel it comfortable and preferable to use them, have high information richness, and include feedback features.
Pedagogical Approach	• Use experiential and collaborative learning approaches (group-oriented approach, community-centred content, collaborative learning, and experiential and communication-based evaluation). • Use instrumental learning (encompasses techniques: operant learning and shaping) and social learning (encompasses mediational processes: exposure, attention, comprehension, acceptance, and retention). • Promote flow and ownership in learning (use of learning materials that suit the audience's current knowledge and skill levels, provide positive feedback on learning progress, give autonomy over learning, make the learning experience entertaining, and incorporate social interaction). • Consider learning as a gradual and long-term process that progresses in multiple stages, and use persuasion techniques (logic, emotion, morals and ethics, well-being, feeling of security, and rationality). • Use a constructivism approach (active participation and learning by doing) using tools like serious games, and online tools (to address misconceptions). • Use the threshold concepts (understand the learners, tailor the learning experience, and incorporate peer-based support) to provide a personalised learning experience. • Provide relevant and role-specific examples, up-to-date content, short modules, flexible learning modes, multiple delivery methods, and a grading system for an evaluation, • Use various techniques to make the teaching and learning more effective (e.g., which use media suitable for the learners, include feedback interventions, provide autonomy in learning processes/flexible learning modes, are entertaining to learn, involve social interactions, provides role-specific and relevant examples, use up-to-date content, use short and comprehensible modules, and implement multi-delivery methods).

Persuasion Principle	• Provide plausible arguments on how the audience benefits by changing security attitudes or behaviour, using attention-grabbing messages (entertaining content or raising mild fear may work). • Use a credible (trustworthy and expert) communicator, and tailor the message and communication channel to the audience (consider the audience's pre-existing attitude, personality traits, and personal relevance). • Implement Cialdini's six principles of persuasion (reciprocation, commitment and consistency, social proof, liking, authority, and scarcity) for message framing and delivery to increase the persuasive effect. • Utilise the MINDSPACE (Messenger, Incentives, Norms, Defaults, Salience, Priming, Affect, Commitments, and Ego) framework but consider the criteria of the EAST framework to motivate the audience to adopt security behaviour. • Provide structurally organised content and enforce effortful responses.
Nudge Theory	• Use coping appraisal message, combined message (both threat and coping appraisals message), male anthropomorphic characters, and loss/gain message as message nudges, • Design (implementing the concepts of usable security and message framing) suitable digital nudges to minimise or address the influence of various psychological biases. • Implement the EAST (easy, attractive, social, and timely) framework to design and apply digital nudges.
Cultural and Cognitive Biases	• Minimise the effect, address, and utilise (whichever is possible) of these biases: Affect Heuristic, Aggregate bias, Anchoring effect, Authority bias, Availability heuristic, Bandwagon effect, Choice architecture, Cognitive overloading, Correspondence bias or attribution effect, Confirmation bias, Congruence heuristic, Context of scarcity, Framing effect, Hassle factor, Habituation, Hyperbolic time discounting, Loss aversion, Optimism bias, Present bias, Priming, Status quo bias, and Cultural biases.
Incentive	• Use incentives that are valuable for the audience in the given time and context. • Prefer intrinsic incentives over extrinsic incentives for long-term behavioural change. • Use extrinsic incentives when an urgent change is required.
Usable Security	• Make security products, processes, and guidelines usable.
Human Trait	• Use relevant demographic information; personality, cognition, and behavioural traits; and decision-making styles to personalise cybersecurity awareness (CSA) initiatives.

Table 1: List of Factors to Motivate CSB Adoption or Change [1]

This list has two primary problems:

- Many factors and recommendations are semantically overlapping.
- There are too many factors and recommendations for practical implementation.

4 Delphi method

The Delphi method is a systematic and qualitative method of forecasting by collecting opinions from a panel of experts through multiple rounds of questionnaires sent to them [8]. After each round of questionnaires, the experts are presented with an aggregated summary of the last round, allowing each expert to adjust their answers according to the group response in the following round. The study is completed when a predefined stop criterion is met, for example, the targeted round of questionnaires is completed, a consensus of forecasts is achieved, and the results have achieved the required stability.

Figure 1 lists the general steps of the Delphi method that have been followed in this study. The Delphi method is widely used for forecasting and issue identification or prioritisation. A variant "*ranking-type*" Delphi is widely used to establish group consensus about the relative importance of issues [9] [10]. Since the objective of this study is to determine the significance of each factor for CSB purposes while also identifying the important factors that were left off the list, we believe that the Delphi method could be more suitable for the study.

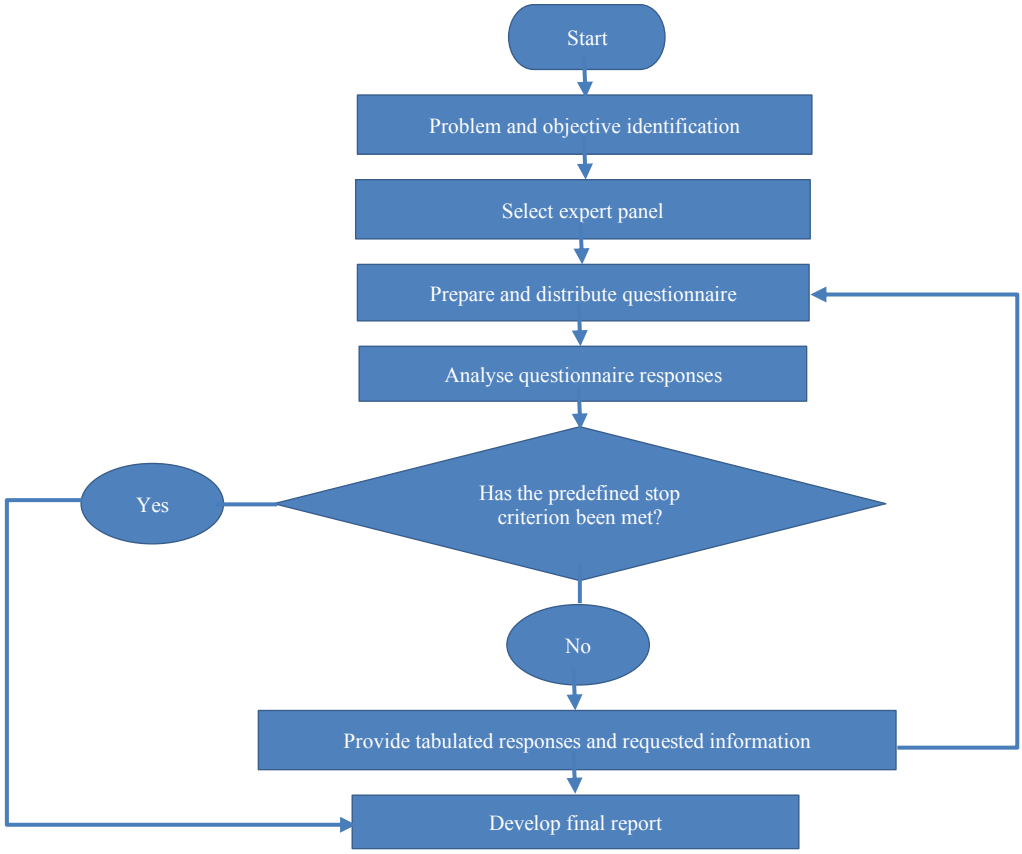

Figure 1: Flowchart for conducting the Delphi method

4.1 Problem and objective identification

The purpose of this study is to improve the effectiveness of CSA, which in other words can be stated as to improve the CSB of people. The D9.18 report [1] resulted in an extensive list of factors that could motivate people to change and adopt CSB and the current study is its follow-up. The major problem with the obtained list is that incorporating all of the suggested factors is difficult in practice. Moreover, the list may have contained less significant factors while at the same time overlooking some critical factors. As a result, the objectives of this study are, first to identify and incorporate any overlooked factors, and then to reduce the list down to only the most significant factors (a maximum of ten factors) in order to make it usable and practically implementable.

4.2 Expert panel selection and profile

The next crucial step is selecting competent experts, or trained specialists who have a thorough understanding of the topic. In general, the nature of research questions determines the size and the constituents of experts, where 10-18 members are recommended for a panel [9]. In this study, we used only one panel of experts, however, these members come from and represent different related disciplines and

professional backgrounds. Since the nature of CSB differs with national culture, this study has a composition of experts from different countries. In order to identify and approach the experts, we used an iterative approach, i.e., contact experts and ask contacts to nominate other experts.

The first round of the survey was completed by 39 experts. However, just 22 of them took part in the survey's second round. We gently reminded the experts who did not respond to the questionnaire via two emails because it was voluntary participation. Due to the time limit for this study, we were unable to wait for all the participants to answer. Unfortunately, the second round of the survey occurred around the autumn break in several countries, which may have contributed to the low response rate.

As a result, we only reviewed and analysed the responses of 22 participants who completed both rounds of the survey. These participants' details are as follows:

- Qualification— 14 participants have PhD degrees, 3 participants are nearing the end of their doctoral studies, and the remaining 5 participants have bachelor's and master's degrees but with extensive professional experiences.
- Discipline— 12 from ICT and cybersecurity, 4 from education and educational technology, 4 from psychology, and the remaining 2 from law and social science.
- Nationality— 5 from Slovenia, 5 from Finland, 4 from Greece, 3 from Norway, and 1 from each of the following countries: Australia, China, Denmark, Germany, and the United Kingdom.
- Profession— 15 participants work in academic organisations, for example, as researchers, lecturers, and professors, and the remaining 7 participants work in non-academic organisations, for example, as psychologists, lawyers, designers, and human resource advisors.

4.3 Questionnaire design and distribution

The questionnaires for the two rounds of the survey are primarily based on the results of LR performed in the D9.18 report, which are also shown in Table 1: List of Factors to Motivate CSB Adoption or Change [1]

.

The questionnaire for the first-round survey (Annex A : Delphi questionnaire- Round 1) has seven closed-end questions and one open-ended question. The closed-ended questions employed a 5-point Likert scale, and the participants were asked to rank the importance of techniques and strategies from various disciplines for CSB adoption and change purposes. The open-ended question asked the participants if there were any relevant techniques and strategies from the excluded discipline that could help with CSB adoption and change.

The second-round survey questionnaire (Annex B : Delphi questionnaire- Round 2) contains 14 questions, with each closed-ended question followed by an open-ended question. The closed-ended questions list out factors from different disciplines that can motivate people to adopt or change CSB. The participants were asked to select only factors that are must-haves (i.e., most important). The open-ended questions asked the participants to input factors from the respective discipline that are important to motivate people to adopt and change CSB if there are any missed ones.

The online surveys were created using Nettskjema [11] from the University of Oslo. In each round, the survey link was then emailed to the selected experts, along with a response deadline. The original deadline for responding to each round was two weeks; however, due to requests from some participants, the period was extended by one week. As a result, each round of the survey received a three-week response period. Those who did not respond on time received follow-up emails as reminders. Participants in the second-round survey were also provided with the outcomes of the first-round survey.

4.4 Questionnaire responses

4.4.1 First round survey

Table 2 and Table 3 summarise the results of the first-round survey, with 39 participants and 22 participants (who also participated in the second-round survey) respectively. In both tables, Q represents the closed-ended questions (as listed in Annex A : Delphi questionnaire- Round 1) and the value indicates the percentage of participants' responses.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Very Important	58.8%	33.3%	30.8%	28.2%	33.3%	43.6%	53.8%
Important	33.3%	48.7%	33.3%	46.2%	48.7%	46.2%	28.2%
Moderately Important	12.8%	15.4%	28.2%	15.5%	15.4%	10.3%	10.3%
Slightly Important	0%	2.6%	7.7%	10.3%	2.6%	0%	7.7%
Not Important	0%	0%	0%	0%	0%	0%	0%

Table 2: Outcomes of the first-round survey (with 39 participants)

	Q1	Q2	Q3	Q4	Q5	Q6	Q7
Very Important	54.0%	27.0%	32.0%	27.0%	27.0%	45.0%	45.0%
Important	32.0%	50.0%	32.0%	45.0%	59.0%	41.0%	23.0%
Moderately Important	14.0%	18.0%	27.0%	14.0%	14.0%	14.0%	18.0%
Slightly Important	0%	5.0%	9.0%	14.0%	0%	0%	14.0%
Not Important	0%	0%	0%	0%	0%	0%	0%

Table 3: Outcomes of the first-round survey (with 22 participants)

More than 60% of the participants responded that strategies and techniques from all given disciplines are either *very important* or *important* (above the neutral option of *moderately important*) in motivating CSB adoption and change (highlighted using light blue colour in the tables). The given disciplines are as follows:

- Psychology and human behaviour (86%)
- Persuasion theory (77%)
- Nudge theory (64%)
- Cognitive theory (72%)
- Framing theory (86%)
- Communication theory (86%)
- Pedagogic theory (68%)

Further, they cited personalisation, humour, storytelling, previous experience, and a sense of individual responsibility to be essential factors that increase CSB adoption and change.

Interestingly, the results showed that all the disciplines deduced through LR are important for motivating CSB adoption and change. Most respondents rated the *nudge theory* as *moderately important* among the listed disciplines. However, if we look at the results of the second-round survey, we see that three of the four factors from the *nudge theory* have been rated *must-haves* by more than 60% of the respondents. So, one possible explanation for this disparity in results is that the first-round survey's question number 3 was poorly phrased, which may have hindered participants' interpretation and understanding of the question. The participants got detailed factors in the second-round survey, which may have clarified their grasp of the nudge theory.

4.4.2 Second round survey

The outcomes of the first-round survey led to the second round of surveying. The first-round survey established that strategies and techniques from all the given disciplines are important to motivate CSB adoption and change. In the second-round survey, the participants had to select only "*must-haves*" factors (techniques and strategies) that can motivate CSB adoption and change. The listed factors are from the above-mentioned disciplines. The outcomes of the second-round survey are summarised in Table 4**Error! Reference source not found.**.

	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11	F12	F13	N
Q1	81.8%	50%	77.3%	40.9%	63.6%	50.0%	45.5%							0%
Q2	77.3%	54.5%	59.1%	54.5%	31.8%	63.6%								0%
Q3	72.7%	18.2%	63.6%	72.7%										4.5%
Q4	54.5%	81.8%	63.6%	45.5%	68.2%	18.2%	63.6%	90.9%						0%
Q5	72.7%	90.9%	45.5%	72.7%	68.2%	100%	54.5%	31.8%						0%
Q6	40.9%	77.3%	86.4%	77.3%	45.5%	68.2%	72.7%							0%
Q7	68.2%	50%	59.1%	54.5%	50%	40.9%	45.5%	77.3%	31.8%	31.8%	40.9%	31.8%	81.8%	0%

Table 4: Outcomes of the second-round survey

In the table, Q represents the closed-ended questions (as listed in Annex B : Delphi questionnaire- Round 2) and F indicates the factors (options) provided in each question. In addition, N indicates the "*None of the above*" option, and the value represents the percentage of participants' responses. The following factors were chosen by more than 60% of respondents as "*must-haves*", and these factors have been denoted by PF (pertinent factor) for later use in the report:

Behavioural constructs

- **PF1:** Inform and if possible, demonstrate through real-life examples, how a threat could seriously harm the audience if it succeeds (perceived severity). However, do not assuage or exaggerate the threat or be alarmist causing an unhealthy level of fear in the audience—an uncontrolled level of fear is ideally not good for healthy decision-making.
- **PF2:** Clearly communicated the security behaviour expected from the audience and promote security behaviour as norms or social etiquette that everyone follows (subjective norms). However, the security behaviour should be realistic and doable to the audience.

- **PF3:** Make the audience aware of the intrinsic and extrinsic harms, e.g., stress, reputational damage, monetary losses, fines, sanctions, and punishments, the audience may suffer if people do not comply with security rules and policies or avoid/fail to execute good security behaviour (perceived cost of non-compliance).

Persuasion strategies

- **PF4:** The source of security information, i.e., messenger, is someone whom the audience is most likely to listen to and trust, e.g., someone with authority (i.e., utilise authority bias—people tend to obey the request of figures who are authoritative, credible, and knowledgeable experts), or similar characteristics (i.e., utilise liking principle — people tend to like and listen to someone who is similar in terms of interests, attitudes, and beliefs).
- **PF5:** In organisations, leadership and top management's interest and participation in CSA initiatives are imperative to motivate employees.

Usability and nudging techniques

- **PF6:** Regularly remind the audience of cybersecurity issues and their potential impacts on individuals, organisations, and society, through different means.
- **PF7:** Make non-compliance and poor security choices the least lucrative. Risky behaviour is made difficult to undertake while the recommended security choices/ settings ought to be preselected by default (i.e., utilise default bias—people tend to go with the flow of pre-set security options).
- **PF8:** CSA messages focus on coping methods, i.e., information on how to minimise exposure to risk (people fail to behave securely because they do not know what secure behaviour entails).

Framing strategies

- **PF9:** Make important security information (i.e., the main message) more prominent or salient through, e.g., strategically positioning it, repeating the information, and connecting the information with known things and events.
- **PF10:** Personalise the security message for the audience (that meets their needs and requirements). And in order to do so, utilise demographic factors like age group, gender, national cultural values, educational level, academic major, and cybersecurity experience.
- **PF11:** Use positive phrasing and framing for the security message formation (since positive messages are more persuasive, and an awareness message is preferably succinct so telling what to do rather than what not to do could be more logical).
- **PF12:** Use a compelling security message with a clear call for doable actions that do not obstruct the audience's primary task, in other words, avoid suggesting actions that the audience could not attain due to their lack of/ limited knowledge and skills (i.e., address hassle factor— security demands that are irritating, frustrating, and distressing may impact people's security decisions).
- **PF13:** Use simple and clear language to compose security messages (e.g., using familiar vocabulary, and non-technical terms).

Communication strategies

- **PF14:** The messenger should be someone with authority or expertise, whom the audience would listen to and trust for security information.
- **PF15:** The security message content is well-organised contributing to its understandability and memorability.
- **PF16:** The security message is factually correct (i.e., valid security practices).

- **PF17:** The security message is polite and courteous (i.e., unbiased, and does not hurt any community or nationality, for example, by blaming them to be responsible for a certain cyberattack).
- **PF18:** The security message is clear (i.e., easy to understand, with a clear goal and concrete wordings) and concise (i.e., brief, to the point, and comprehensible).

Pedagogical strategies

- **PF19:** Start with simple security tasks (or issues) and gradually increase the task's complexity as the audience gain mastery of them.
- **PF20:** Use real-life examples to explain security issues (e.g., harms from a threat and the protection mechanisms).
- **PF21:** Connect the security learning process with the individuals' interest (e.g., use serious games for young game lovers).
- **PF22:** Use experiential learning for security teaching (where the learning is done by doing or learning by hands-on experience and reflection).
- **PF23:** Use cognitive (or brain) friendly strategies for security teaching and learning activities (e.g., use real-life cases, storytelling, and games).

Cognitive biases

- **PF24:** Affect heuristic—People underestimate, or overestimate risks and costs associated with security based on whether they like or dislike it, respectively.
- **PF25:** Habituation—People can become less responsive to a security stimulus if it is repeated or presented for a prolonged time.
- **PF26:** Status quo bias—People tend to prefer things to stay as they are, which leads them to continue with the default security option provided to them.

The open-ended questions elicited suggestions such as employing serious games, real-life cases/examples, and a problem-based learning approach, all of which we believe are redundant to what the closed-ended questions covered. Furthermore, the participants suggested CSB initiatives be considerate of social norms and national culture, which again is redundant to what has been covered in the closed-ended questions.

An intriguing proposal that the questionnaire did not include is to portray cybersecurity as a social corporate responsibility in organisations, as well as ethical/moral ways of serving society in general. Treating cybersecurity protection as corporate social responsibility is frequently proposed for organisations; however, it is unclear how much of an impact this would have on an individual's CSB.

5 Analysis of responses and resulting list of factors

Based on the percentage of participants who thought the factors are "*must-haves*", the factors can be arranged as follows:

- PF18 (100%)
- PF13, PF15 (90.0%)
- PF20 (86.4%)
- PF1, PF9, PF26 (81.8%)
- PF2, PF4, PF19, PF21, PF25 (77.3%)
- PF6, PF8, PF14, PF16, PF23 (72.7%)
- PF11, PF17, PF22, PF24 (68.2%)
- PF3, PF5, PF7, PF10, PF12 (63.6%)

In this, many framing-related variables were chosen as "*must-haves*" by most participants. This could be due to the fact that the persuasive effect of communication is heavily influenced by its message framing [12]. Here, we do not want to go into detail on message framing because it has already been extensively explored in our prior reports [1] [13] and a publication [14].

The obtained factors could be further condensed into the following categories:

Management support for and participation in cybersecurity activities (PF6)

In an organisation, the leadership or top management should be interested in and participate in cybersecurity-related activities. Their interest and participation are critical to staff motivation (i.e., *leading by example*) as well as the long-term viability of cybersecurity initiatives.

Cybersecurity to be an ongoing process (PF7)

People should be regularly reminded of cybersecurity issues and their potential impacts on individuals, organisations, and society, through different means. This is because people tend to forget gained knowledge over time (the *forgetting curve* conveys that the learned information is lost over time if the learners do not revisit or establish connections to it).

Cybersecurity to be a social norm (PF2, PF8, PF24, PF26)

Cybersecurity behaviour should be promoted as social norms or etiquette that everyone follows (i.e., to address *affect heuristic*—people underestimate, or overestimate risks and costs associated with security based on whether they like or dislike it, respectively). All individuals should know the security behaviour expected from them. However, the expectations must be realistic and doable for the people targeted. In this effort to establish cybersecurity behaviour as a social norm, the following approaches could be helpful:

- *Social proof* (i.e., people copy the actions of others in an attempt to undertake behaviour in a given situation) approaches to prove cybersecurity is a norm.
- *Security by default,* where non-compliance and poor security choices are made the least lucrative. This also means the risky behaviour is made difficult to undertake while the recommended security choices/ settings ought to be preselected by default (i.e., utilise *status quo bias*—people tend to prefer things to stay as they are, which leads them to continue with the default security option provided to them).

Incentives for cybersecurity actions (PF1, PF3)

People should be informed and if possible, demonstrated through real-life examples, how a security threat could seriously harm them if it succeeds (i.e., to utilise *incentive effect*—rewards and penalties-motivated outcome). These incentives could be intrinsic and extrinsic harms, e.g., stress, reputational damage, monetary losses, fines, sanctions, and punishments, that people may suffer if they do not comply with security rules and policies or avoid/fail to execute good security behaviour (i.e., to utilise *loss aversion bias*—people prefer avoiding losses to acquiring equivalent gain). At the same time, however, it is suggested not to assuage or exaggerate the threat or be alarmist causing an unhealthy level of fear in the audience—after all an uncontrolled level of fear is ideally not good for healthy decision-making.

Persuasive framing of cybersecurity messages (PF9, PF11, PF12, PF13, PF14, PF15, PF16, PF17, PF18)

To produce an impactful security message, it should be:

- factually correct (i.e., convey valid security practices),
- composed in simple and clear language (e.g., using familiar vocabulary, and non-technical terms),
- clear in context (i.e., easy to understand, with a specific goal, and concrete wordings),
- concise (i.e., brief, to the point, and comprehensible),

- well-organised contributing to its understandability and memorability,
- with a clear call for doable actions that do not obstruct people's primary task, in other words, avoid suggesting actions that the audience could not attain due to their lack of/ limited knowledge and skills (i.e., address *hassle factor*— security demands that are irritating, frustrating, and distressing may impact people's security decisions),
- personalised for the target group of people (that meets their needs and requirements, and considers demographic factors like age group, gender, national cultural values, educational level, academic major, and cybersecurity experience),
- focused on coping methods, i.e., information on how to minimise exposure to risk (people fail to behave securely because they do not know what secure behaviour entails)
- polite and courteous (i.e., unbiased, and does not hurt any community or nationality, for example, by blaming them to be responsible for a certain cyberattack).
- positive phrasing and framing should be used for the security message formation (since positive messages are more persuasive, and an awareness message is preferably succinct so telling what to do rather than what not to do could be more logical)

Effective communication of cybersecurity messages (PF4, PF5, PF19, PF20, PF21, PF22, PF23)

The two critical aspects of communicating a cybersecurity message are the messenger and the delivery approach.

The source of cybersecurity information, i.e., the messenger, should be someone whom the audience is most likely to *listen to* and *trust*. Such an individual could be someone with authority (i.e., to *utilise authority bias*—people tend to obey the request of figures who are authoritative, credible, and knowledgeable experts), or someone with similar characteristics such as peers (i.e., to utilise *liking principle*—people tend to like and listen to someone who is similar in terms of interests, attitudes, and beliefs).

The approaches used for message delivery should

- start with simple security tasks (or issues) and gradually increase the task's complexity as the audience gain mastery of them,
- use cognitive (or brain) friendly strategies (e.g., use real-life cases, storytelling, and games),
- connect the security learning process with the individuals' interest (e.g., use serious games for young game lovers), and
- use experiential learning for security teaching (where the learning is done by doing or hands-on experience and reflection).

User-friendly presentation of cybersecurity messages (PF10, PF25)

In order to result in a user-friendly presentation,

- the important security information (i.e., the main message) should be made more prominent or salient through, e.g., strategically positioning it, repeating the information, and connecting the information with known things and events, and
- address negligence (e.g., caused due to *habituation*—people can become less responsive to a security stimulus if it is repeated or presented for a prolonged time).

6 Conclusions

CSA entails persuading people to adopt a new behaviour (i.e., good practices) and changing their existing behaviour (i.e., bad practices). This requires more than simply informing people what to do and what not to

do; people must acknowledge that the information is significant, comprehend how they should respond, and be willing to do so in the face of competing demands [15]. Prompting these changes in people's knowledge and intentions is best accomplished through the use of applicable techniques and strategies from many disciplines [15] [16]. Some strongly recommended factors for the purpose (i.e., CSB adoption and change) are as follows:

- Management support for and participation in cybersecurity activities
- Cybersecurity to be an ongoing process
- Cybersecurity to be a social norm
- Incentives for cybersecurity actions
- Persuasive framing of cybersecurity messages
- Effective communication of cybersecurity messages
- User-friendly presentation of cybersecurity messages

Finally, many viable approaches to achieving these aspects have been discussed in our previous deliverable report D3.19 [13] and conference paper [14].

7 References

[1] S. Chaudhary, "Awareness effectiveness study 2," CyberSec4Europe, 2022.

[2] T. Mashiane and E. Kritzinger, "Cybersecurity Behaviour: A Conceptual Taxonomy," in *O. Blazy and C. Y. Yeun (Eds.): WISTP 2018*, Springer Nature Switzerland, 2019, p. 147–156.

[3] S. Chaudhary, V. Gkioulos and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity,* vol. 8, no. 1, 2022.

[4] Y. Hong and S. Furnell, "Understanding cybersecurity behavioral habits: Insights from situational support," *Journal of Information Security and Applications,* vol. 57, March 2021.

[5] M. Warkentin, A. C. Johnston and J. Shropshire, "The influence of the informal social learning environment on information privacy policy compliance efficacy and intention," *European Journal of Information Systems,* vol. 20, no. 3, pp. 267-284, 2011.

[6] J. M. Stanton, K. R.Stam, P. Mastrangelo and J. Jolton, "Analysis of end user security behaviors," *Computers & Security,* vol. 24, no. 2, pp. 124-133, March 2005.

[7] R. M. Bergner, "What is behavior? And so what?," *New Ideas in Pscyhology,* vol. 29, no. 147–155, 2011.

[8] CFI, "Delphi Method," 7 November 2022. [Online]. Available: https://corporatefinanceinstitute.com/resources/economics/delphi-method/. [Accessed 25 November 2022].

[9] C. Okoli and S. D. Pawlowski, "The Delphi method as a research tool: an example, design considerations and applications," *Information & Management,* vol. 42, pp. 14-29, 2004.

[10] R. Schmidt, K. Lyytinen, M. Keil and P. Cule, "Identifying Software Project Risks: An International Delphi Study," *Journal of Management Information Systems,* vol. 17, no. 4, pp. 5-36, 2001.

[11] University of Oslo, "Nettskjema," [Online]. Available: https://www.uio.no/english/services/it/adm-services/nettskjema/. [Accessed 31 October 2022].

[12] S. M. Smith and R. E. Petty, "Message Framing and Persuasion: A Message Processing Analysis," *Personality and Social Psychology Bulletin,* vol. 22, no. 3, pp. 257-268, March 1996.

[13] S. Chaudhary, S. Pape, M. Kompara, G. Kavallieratos and V. Gkioulos, "D3.19 Guidelines for Enhancement of Societal Security Awareness," CyberSec4Europe, Brussels, Belgium, 2022.

[14] S. Chaudhary, M. Kompara, S. Pape and V. Gkioulos, "Properties for Cybersecurity Awareness Posters' Design and Quality Assessment," in *17th International Conference on Availability, Reliability and Security*, Vienna, Austria, August 2022.

[15] M. Bada, A. M. Sasse and J. R. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," in *International Conference on Cyber Security for Sustainable Society*, Coventry, UK, 2015.

[16] P. Dolan, M. Hallsworth, D. Halpern, D. King and I. Vlaev, "MINDSPACE-Influencing behaviour through public policy," Institute for Government, London, UK, 2015.

Annex A : Delphi questionnaire- Round 1

Thank you for participating in this survey. Your participation in the survey and your individual responses will be strictly confidential to the research team and will not be divulged to anyone outside, including other survey participants. The data gathered within this survey is for use only as part of the CyberSec4Europe research project (https://cybersec4europe.eu/).

The purpose of this study is to increase the effectiveness of **CYBERSECURITY AWARENESS INITIATIVES**. And cybersecurity awareness initiatives must focus on behaviour change rather than merely increasing cybersecurity knowledge if they are to have a significant impact.

In order to achieve this, the study aims to identify the most relevant (or must-have) factors that must be taken into consideration in order to encourage cybersecurity behaviour change. The following survey is stage X of a Delphi questionnaire. Please answer these questions to the best of your knowledge.

For more information on the Delphi method of survey research, please visit: https://www.projectsmart.co.uk/tools/delphi-technique-a-step-by-step-guide.php

Once we have received responses from all participants, we will collect and summarize the findings and formulate the next iteration of the questionnaire.

If you have any questions about this study now or at any time, please do not hesitate to contact Sunil Chaudhary at sunil.chaudhary@ntnu.no

PERSONAL INFORMATION

Name:

Organization:

Email:

QUESTIONNAIRE: ROUND 1

1. **How important is the application of psychological and behavioural strategies (e.g., components of behavioural theories, persuasion principles, nudging techniques, and cognitive biases) in order to encourage cybersecurity behaviour adoption/change?**

Not Important	Slightly Important	Moderately Important	Important	Very important

2. **How important is the application of persuasion principles (e.g., reciprocation, commitment, social proof, scarcity) in order to encourage cybersecurity behaviour adoption/change?**

Not Important	Slightly Important	Moderately Important	Important	Very important

3. **How important is the application of nudging techniques (e.g., warning or appraisal message, hassle factor, reminder, block-off time) in order to encourage cybersecurity behaviour adoption/change?**

Not Important	Slightly Important	Moderately Important	Important	Very important

4. **How important is the application (and address whichever is relevant) of cognitive biases (e.g., confirmation bias, optimism bias, correspondence bias, anchoring effect) in order to encourage cybersecurity behaviour adoption/change?**

Not Important Slightly Important Moderately Important Important Very important

5. **How important is the application of message framing strategies (e.g., information selection, information salience, information personalization, descriptive/prescriptive format message) in order to encourage cybersecurity behaviour adoption/change?**

Not Important Slightly Important Moderately Important Important Very important

6. **How important is the application of communication strategies (e.g., trustworthy communicator, vertical/horizontal communication, appropriate communication medium, features of language) in order to encourage cybersecurity behaviour adoption/change?**

Not Important Slightly Important Moderately Important Important Very important

7. **How important is the application of pedagogical strategies (e.g., experiential learning, collaborative learning, instrumental learning, social learning) in order to encourage cybersecurity behaviour adoption/change?**

Not Important Slightly Important Moderately Important Important Very important

8. **Is there any other relevant strategy or technique that has been missed out but can be play role in order to encourage cybersecurity behaviour adoption/change? Please mention them.**

……
……
……
……

Annex B : Delphi questionnaire- Round 2

Thank you very much for participating in stage 1 and the current stage 2 of the Delphi survey.

This is stage 2 of the survey. Once again, your participation in the survey and your individual responses will be strictly confidential to the research team and will not be divulged to anyone outside, including other survey participants. The data gathered within this survey is for use only as part of the CyberSec4Europe research project (https://cybersec4europe.eu/).

The purpose of this study is to increase the effectiveness of **CYBERSECURITY AWARENESS INITIATIVES**. And cybersecurity awareness initiatives must focus on **BEHAVIOR CHANGE** rather than merely increasing cybersecurity knowledge if they are to have a significant impact. In order to achieve this, the study aims to identify the **MOST RELEVANT (MUST-HAVES)** factors that have to be taken into consideration in order to encourage cybersecurity behaviour change. The listed factors are the suggestions that have been made by different past studies.

For more information on the Delphi method of survey research, please visit: https://www.projectsmart.co.uk/tools/delphi-technique-a-step-by-step-guide.php

Once we have received responses from all participants, we will collect and summarize the findings and formulate the next iteration of the questionnaire. The summary of the feedback from stage 1 has been sent to you as an email attachment.

Please answer these questions to the best of your knowledge. The questionnaire has been designed in as simple and understandable language as possible. If you have any questions about this study now or at any time, please do not hesitate to contact Sunil Chaudhary at sunil.chaudhary@ntnu.no

PERSONAL INFORMATION

Name:

Organization:

Email:

QUESTIONNAIRE: ROUND 2

1. **Select the behavioural constructs that are *must-haves* to motivate cybersecurity behaviour change/adoption. (Multiple options can be selected.)**
   - Inform and if possible, demonstrate through real-life examples, how a threat could seriously harm the audience if it succeeds (***perceived severity***). However, do not assuage or exaggerate the threat or be alarmist causing an unhealthy level of fear in the audience—an uncontrolled level of fear is ideally not good for healthy decision-making.
   - Instil a sense of self-efficacy (***response efficacy***—the belief that the recommended security action will lead to the removable or at least a reduction of the threat; ***self-efficacy*** —an individual's perception of the audience's own ability to successfully exhibit the recommended security behaviour) in the audience through different means, e.g., mastery experiences, and persuasion.
   - Clearly communicated the security behaviour expected from the audience and promote security behaviour as norms or social etiquette that everyone follows (***subjective norms***). However, the security behaviour should be realistic and doable to the audience.
   - Make the audience aware of the intrinsic and extrinsic benefits or gains, e.g., rewards, praise, and safeguarding of resources, from complying with security policies and by performing good security behaviour (***perceived benefits of compliance***).

- Make the audience aware of the intrinsic and extrinsic harms, e.g., stress, reputational damage, monetary losses, fines, sanctions, and punishments, the audience may suffer if people do not comply with security rules and policies or avoid/fail to execute good security behaviour (***perceived cost of non-compliance***).
- Inform the audience of the ***certainty of sanctions***, and the magnitude of sanctions they would suffer for non-compliance (***perceived severity of sanctions***). However, the intensity of sanctions should be proportionate and not too harsh.
- Reduce the efforts and other costs required to comply with security policies and perform recommended security behaviour (***response cost***—all costs associated with performing the recommended security behaviour or action; ***perceived cost of compliance*** —monetary and non-monetary costs that could incur by complying with security policies and perform security behaviour).

2. Please specify if any behavioural construct relevant to the purpose is missing.

……
……
……
……

3. Select the persuasion strategies that are *must-haves* to motivate cybersecurity behaviour change/adoption. (Multiple options can be selected.)

- The source of security information, i.e., messenger, is someone whom the audience is most likely to listen to and trust, e.g., someone with authority (i.e., utilize ***authority bias***—people tend to obey the request of figures who are authoritative, credible, and knowledgeable experts), or similar characteristics (i.e., utilize ***liking***- people tendency to like someone who is similar in terms of interests, attitudes, and beliefs).
- Provide incentives, ideally intrinsic ones, to motivate the audience to change/adopt good cybersecurity behaviour for the long term (i.e., utilize ***reciprocation***—people tend to give something in return). However, the incentives should be immediate and connected to something that makes sense and matters to the audience in the given time and context.
- Promote good security behaviour as social etiquette or norms. Let everyone know who else, e.g., peers or people in the authority whom others emulate, practice security behaviour by commending them publicly (i.e., utilize ***social proof***—people tend to imitate the behaviour of other people).
- Make the audience aware of, preferably, the potential harms from the non-compliance to security policies and behaviour over the potential gains from compliance to security policies and behaviour (i.e., utilize ***loss aversion***—people tend to perceive loss as psychologically or emotionally more severe than an equivalent gain).
- Connect cybersecurity to other tangible issues that can stimulate the audience much more than cybersecurity itself. However, the issue should be visible and have gained momentum, for example, terrorists using cybercrime to fund their malicious activities.
- In organizations, leadership and top management's interest and participation in cybersecurity awareness initiatives are imperative to motivate employees.

4. Please specify if any persuasion strategy relevant to the purpose is missing.

……
……
……
……

5. **Select the usability and nudging techniques that are must-haves to motivate cybersecurity behaviour change/adoption. (Multiple options can be selected.)**
   - Regularly remind the audience of cybersecurity issues and their potential impacts on individuals, organizations, and society, through different means.
   - Invoke a mild fear enough to attract the audience's attention toward cybersecurity issues and generate information-seeking behaviour. However, it should avoid causing an unnecessary level of fear.
   - Make non-compliance and poor security choices the least lucrative. Risky behaviour is made difficult to undertake while the recommended security choices/ settings ought to be preselected by default (i.e., utilize ***default bias***—people tend to go with the flow of pre-set security options).
   - Cybersecurity awareness messages focus on coping methods, i.e., information on how to minimize exposure to risk (people fail to behave securely because they do not know what secure behaviour entails).

6. **Please specify if any usability and nudging technique relevant to the purpose is missing.**

……
……
……
……

7. **Select the framing strategies that are *must-haves* for cybersecurity awareness messages framing. (Multiple options can be selected.)**
   - Communicate only security information that the audience needs to know, not all security information that could generally be beneficial to know (there can be a load of security information that is good to know and including all could cause ***cognitive overload***).
   - Make important security information (i.e., the main message) more prominent or salient through, e.g., strategically positioning it, repeating the information, and connecting the information with known things and events.
   - Personalize the security message for the audience (that meets their needs and requirements). And in order to do so, utilize demographic factors like age group, gender, national cultural values, educational level, academic major, and cybersecurity experience.
   - Use descriptive format (i.e., description of cybersecurity knowledge used in daily life) for the security message presentation except for organizational purposes where prescriptive format (i.e., action-guiding steps on how and when the cybersecurity knowledge is used) may require. There is a risk of indoctrination in a prescriptive format, which may hinder the audience from rational thinking.
   - Use positive phrasing and framing for the security message formation (since positive messages are more persuasive, and an awareness message is preferably succinct so telling what to do rather than what not to do could be more logical).
   - Provide the complete security message that the target audience needs to be informed about and, if applicable to act (e.g., state the security problem/threat, characteristics used to identify the

problem/threat, the impact of the problem/threat if not acted upon, and preventive/ mitigative/ responsive actions).

- Use a compelling security message with a clear call for doable actions that do not obstruct the audience's primary task, in other words, avoid suggesting actions that the audience could not attain due to their lack of/ limited knowledge and skills (i.e., address ***hassle factor***— security demands that are irritating, frustrating, and distressing may impact people's security decisions**).**
- Use simple and clear language to compose security messages (e.g., use familiar vocabulary, non-technical terms).

8. Please specify if any framing strategy relevant to the purpose is missing.

……
……
……
……

9. Select the communication strategies that are must-haves to convey cybersecurity awareness messages. (Multiple options can be selected.)

- The messenger should be someone with authority or expertise, whom the audience would listen to and trust for security information.
- The security message content is well-organized contributing to its understandability and memorability.
- The security message targets a specific audience group at a time. A generic message would not attract the audience's attention or disinterest them.
- The security message is factually correct (i.e., valid security practices).
- The security message is polite and courteous (i.e., unbiased, and does not hurt any community or nationality, for example, by blaming them to be responsible for a certain cyberattack).
- The security message is clear (i.e., easy to understand, with a clear goal and concrete wordings) and concise (i.e., brief, to the point, and comprehensible).
- The communication media used to deliver security messages best fit the message types and be of interest to the audience (e.g., serious games for the young age group).
- The communication media used to deliver security messages have a credible channel for two-way communication. This will allow the interested audience to ask questions and provide feedback, i.e., support interactive communication.

10. Please specify if any communication strategy relevant to the purpose is missing.

……
……
……
……

11. Select pedagogical strategies that must have to improve the impact of cybersecurity teaching and learning activities. (Multiple options can be selected.)

- Group the learners based on learners' pre-existing beliefs/attitudes and security expertise levels so that information and communication strategies could be targeted more specifically to the group.

- Start with simple security tasks (or issues) and gradually increase the task's complexity as the audience gain mastery of them.
- Use real-life examples to explain security issues (e.g., harms from a threat and the protection mechanisms).
- Connect the security learning process with the individuals' interest (e.g., use serious games for young game lovers).
- Use collaborative learning for security teaching (where groups of two or more learners work together to solve problems, complete tasks, or learn new concepts).
- Use experiential learning for security teaching (where the learning is done by doing or learning by hands-on experience and reflection).
- Use cognitive (or brain) friendly strategies for security teaching and learning activities (e.g., use real-life cases, storytelling, and games).

12. Please specify if any pedagogy strategy relevant to the purpose is missing.

……
……
……
……

13. Select the cognitive biases and psychological factors that *must* be addressed through cybersecurity awareness means in order to encourage cybersecurity behaviour adoption/change. (Multiple options can be selected.)

- Affect heuristic—**P**eople underestimate, or overestimate risks and costs associated with security based on whether they like or dislike it, respectively.
- Anchoring bias—**P**eople heavily rely on the initial piece of security information given to them; once an anchor is set, the individual's subsequent arguments, estimates, values, and so on may differ from what they would have without the anchor.
- Availability heuristic—**P**eople use security information that comes to mind quickly and easily when making security decisions.
- Bandwagon effect—**P**eople do certain things, good or bad security behaviour, regardless of their own beliefs, simply because other people are doing it.
- Confirmation bias and Congruence heuristic—**P**eople search for, interpret, favour, and recall security information in a way that confirms or supports their prior beliefs or values.
- Ego—**P**eople act in ways that make them feel better about themselves, so they may resist security behaviour change style that can discomfort them.
- Hassle factor—**S**ecurity demands that are irritating, frustrating, and distressing may impact people's security decisions.
- Habituation—**P**eople can become less responsive to a security stimulus if it is repeated or presented for a prolonged time.
- Hyperbolic time discounting and Present bias—**P**eople may choose a smaller-immediate benefit over a large-later award while making security decisions.
- Loss aversion—**P**eople tend to avoid losses over acquiring equivalent gains while making security decisions.
- Optimism bias—**P**eople overestimate the likelihood of encountering positive events and underestimate the likelihood of experiencing negative events in the future while making security decisions.

- Priming—**P**eople's exposure to one security stimulus influences a response to a subsequent security stimulus, without conscious guidance or intention.
- Status quo bias—**P**eople tend to prefer things to stay as they are, which leads them to continue with the default security option provided to them.

14. Please specify if any cognitive bias and psychological factor relevant to the purpose is missing.

……
……
……
……