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

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.18

Awareness Effectiveness Study 2

Document Identification	
Due date	31 May 2022
Submission date	8 Jun 2022
Revision	1.0

Related WP	WP9 T9.4	Dissemination Level	PU
Lead Participant	NTNU	Lead Author	Sunil Chaudhary (NTNU)
Contributing Beneficiaries	NTNU, TDL, ATOS, JAMK, UM	Related Deliverables	D9.13

Abstract: This report provides a more comprehensive list of factors that should be considered to enhance the effectiveness of cybersecurity awareness programmes, in particular, to motivate people to adopt cybersecurity awareness and translate the message (security recommendations) or learned things into actions and behaviour. The list integrates factors from multi-disciplines, namely 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 to make it as inclusive as possible. The results of this study will be beneficial for cybersecurity professionals and organisations who intend to design, develop, and implement cybersecurity awareness programmes. Further, the knowledge might be useful also for those who generate requests for awareness designers as well as anyone who evaluates the effectiveness of the adopted security measures.

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.

The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Executive Summary

The ultimate goal of cybersecurity awareness (CSA) is to bring change in the security knowledge, attitude, and behaviour of people to increase awareness and trust in digital security. However, in reality, often the outcomes of most CSA initiatives get limited to how knowledge gain measured or is talked about. Undoubtedly, knowledge gain is an important step in the awareness initiatives, such as ENISA/EU CSA month and CSA training programs, but without a change in security attitude and behaviour, presumably, it will have no significant value. One of the main reasons behind the failure of most CSA initiatives is their narrow understanding of awareness. CSA is generally considered as a mere delivery of knowledge, whereas in reality, it should be much more than that. In fact, CSA should encompass knowledge application from various disciplines and sectors, including,

- social psychology— e.g., cognitive and cultural biases, and personal traits impact on security decision-making,
- behavioural economics— e.g., incentives impact on security decision making,
- pedagogy— e.g., suitable learning materials, learning techniques, and effective evaluation,
- usability and user experience— e.g., better usability to facilitate security decision making,
- framing theory— e.g., the influence of information presentation on security decision-making,
- communication theory— e.g., communication phenomena necessary for effective message delivery,
- the science of persuasion— e.g., persuasion to learn and act, and so on.

In CSA, change in attitude and behaviour can be best targeted at content design and its delivery (or communication). The main objective of this report is to elicit the factors that could potentially contribute to enhancing the efficacy of content design and its delivery so as to motivate people and companies to adopt CSA and apply or practice correctly the knowledge learned in everyday (personal and professional) life. In order to do so, this study used a non-systematic literature review. The reviewed studies and the elicited factors have been tentatively grouped under the following headings:

- Behavioural theory,
- Framing theory,
- Communication theory,
- Pedagogical approach,
- Social psychology and behavioural economics (persuasion principle, cognitive and cultural biases, nudge theory, and incentive),
- Usable security, and
- Human traits.

Along with the list of factors, the report also provides potential mitigation measures through which those factors could be addressed or utilised in practice for CSA purposes. Upon further analysis of these factors, they are found to target seven features, namely, psychology, enactment, learning, communication, information/ message, usability, and knowledge and skill.

Despite the fact that the list is compiled using a literature review, there is a chance that some important aspects were overlooked and that some factors are no longer relevant. As a result, the list needs to be validated to increase its relevance and practical application. Its validation will be conducted using a Delphi approach with a panel of experts. The validation results will be presented in the third and final deliverable D9.26 of the "*Awareness effectiveness study*" series.

Document information

Contributors

Name	Partner
Sunil Chaudhary	NTNU

Reviewers

Name	Partner
Jozef Vyskoc	VaF
Marco Crabu	ABI Lab
Christine Jamieson	TDL

History

Version	Date	Authors	Comment
0.01	2021-11-08	Sunil Chaudhary	1st Draft
0.02	2022-05-10	Sunil Chaudhary	2nd Draft
0.03	2022-05-13	Sunil Chaudhary	Integrated the reviewers' comments and suggestions
0.04	2022-05-23	Sunil Chaudhary	Integrated the reviewers' comments and suggestions
1.0	2022-05-30	TDL	Additional corrections
1.0	2022-06-08	GUF	Final check, preparation and submission

Table of Contents

List of Figures

List of Tables

List of Acronyms

C	**CSA**	Cybersecurity Awareness
E	**EAST**	Easy, Attractive, Social, and Timely
F	**FUD**	Fear, Uncertainty, and Doubt
G	**GDPR**	General Data Protection Regulation
	GDT	General Deterrence Theory
I	**IS**	Information System
	IT	Information Technology
L	**LR**	Literature Review
M	**MINDSPACE**	Messenger Incentives Norms Defaults Salience Priming Affect Commitments Ego
P	**PMT**	Protection Motivation Theory
S	**SALSA**	Search, Appraisal, Synthesis, and Analysis
	SETA	Security Education, Training, and Awareness
T	**TAM**	Technology Acceptance Model
	TPB	Theory of Planned Behaviour
	TRA	Theory of Reasoned Action
	TV	Television

1 Introduction

Cybersecurity awareness (CSA) is about being mindful or conscious of cybersecurity issues relevant to personal and professional life. It encompasses *a wide range of skills and competencies by involving awareness of the cyber threats, their potential impacts, their prevention and mitigation measures, and more importantly translating the knowledge into action or behaviour for the benefit of the companies and employees*. It is generally done by communicating up-to-date security information and good practices to the target audience through a multitude of ways and formats of resources [1] with an intent to instil proper security procedures and principles in the audience [2]. The information provided is not in-depth but enough to raise a level of scepticism in people when encountering unusual situations online [3] and so to motivate them to act.

1.1 Purpose and Scope

The ultimate goal of CSA activities is to bring positive changes in the cybersecurity *knowledge* (know), *attitude* (feel), and *behaviour* (do) of the audience [4] [5]; however, in reality, they often fail to attain the expected outcomes [6] [7] [8]. As a result, companies continue to incur losses both from cyberattacks and data breaches caused due to employees' errors and negligence, and insufficient resources invested in CSA initiatives. The failure of CSA initiatives is evident in the survey conducted on 1200 company employees who had undergone CSA training offered by their companies in response to COVID-19, where outrageously 61% of the participants failed even a basic security test [9]. Among the different factors, *the most fundamental reason for the failure of most awareness initiatives is not understanding what CSA really is*. CSA has often been considered as a mere act of delivering security information (traditionally *to do* and *not to do*) to the target audience whereas, in reality, it should be much more than that [6] [10] [11] [12] [13]. Sharing information about security issues with a target audience is undoubtedly a critical step in creating a conducive environment for change, however merely by doing this, it is less likely to change the audience's security attitude and behaviour [14]. In addition to delivering information, there are many other crucial aspects of CSA, for example, creating interest and engaging the audience for participation [11], making clear calls for achievable actions [14], and evoking emotion through positive enforcement to act the way it has been suggested [12].

In order to influence the target audiences and improve the possibility of acting securely and as suggested (i.e., in compliance), firstly the individuals have to understand that the information is significant, then comprehend the information on how they ought to respond appropriately, and finally, develop a determination to act in the face of several other demands (where security is rarely the primary concern [15] and asking people to act outside their normal workflow can be seen as an interruption to the primary task [16] [17]) [6]. However, *to cause those feelings in the target audience requires a deep understanding of communicating the complex problems of cybersecurity in a simple and convincing manner with a specific intent to create a long-lasting attitude and behaviour transformation*. And the challenges of effective communication can be best addressed during content design and its delivery. Awareness content design and its delivery will need to consider and leverage concepts from behavioural sciences, psychology, behavioural economics, and many other disciplines to understand [14] [18] [19]. These include how people formulate preconceptions and beliefs, how socio-psychological, economical, and other factors (for example, cognitive and cultural biases, demographics, personality traits, and risk-taking propensity) impact people's decision-making processes, and what roles different motivation techniques (e.g., persuasion techniques, teaching and learning techniques) can play to enhance cybersecurity attitudes and behaviour change.

As anticipated, many studies (discussed in detail in Section 3) have analysed and recommended behavioural and other factors to change cybersecurity attitudes. Indeed, these factors are highly beneficial; however, knowledge from several relevant fields of study, such as communication, health and social awareness, marketing, pedagogy, user experience and usability, and business/management still remains little explored and cannot be ignored, which could potentially contribute to designing effective strategies for security attitude and behaviour transformation. Moreover, those identified behavioural factors are also scattered in different studies and not inclusive enough. So, there is a need for a more comprehensive approach to assessing the problem, thus producing a consolidated and possibly complete list of factors that could impact attitude and behaviour change in CSA. Not to mention, many of these recommended factors remain at a relatively theoretical level and provide limited guidance on how to apply them in actual situations. Hence, this study attempts also to provide practical and usable guidance/mechanisms for applying those factors in actual situations. More specifically, the research gaps this study aims to address are:

i) The past studies have produced several overlapping and non-overlapping sets of recommendations for influencing security attitude and behaviour change, which are likewise dispersed. Thus, they should be consolidated.

ii) Insights and ideas from other disciplines, for example, communication, health and social awareness, marketing, pedagogy, user experience and usability, and business/management might be valuable in CSA and should be researched so that they can be leveraged to influence security attitude and behaviour. Thus, they should be investigated, assessed, and integrated into CSA.

iii) The past studies have recommended factors relevant to security attitude and behaviour change, however, many have not specified how to apply them in real-life situations. Thus, each recommended factor should have practical and usable implementation procedures.

This is the second of three reports of the "*Awareness effectiveness study*" series. The main objective of Task 9.4 is to enhance CSA across industry and society. We believe that the outcomes of this study align with the objective set forth by the task and will contribute to enhancing the effectiveness of CSA in the workplace and society.

1.2 Audience

This study intends to provide a consolidated and complete list of the most relevant factors that can be used for influencing security attitudes and behaviour change. To the best of our knowledge, there is no specific document like this deliverable report that has considered such a broad and holistic approach to address gaps in the cybersecurity culture, specifically the issues in security attitudes and behaviour transformation. The outcomes of this report will be useful for CSA professionals or organisations/ individuals who aim to design, develop, and implement a CSA content or programme. The identified and validated factors can facilitate them in designing more effective and impactful communication of CSA content, which ultimately will improve the overall effectiveness of the CSA programme and its probability of success. Furthermore, the knowledge could be useful for people who make requests for awareness designers, as well as anyone who evaluates the effectiveness of the adopted security measures.

1.3 Document Structure

The report is structured as follows: Section 1 states the research objectives and briefly explains why they are important to investigate. Section 2 provides the methodologies applied to elicit and analyse the factors for influencing security attitude and behaviour change, particularly, a *non-systematic (purposive) literature review* (LR). Section 3 reviews various relevant past studies and presents their main findings tentatively grouped under various appropriate headings. Section 4 presents the consolidated list of factors identified from the LR. Section 5 concludes the report and provides the objective and plan for the third and final deliverable D9.26 of the awareness effectiveness study.

2 Methodology: Non-systematic Literature Review

In order to achieve the objectives, this study used a *non-systematic (purposive) LR*. In simple terms, a non-systematic LR is not obligated to be explicit about the methods used, particularly the search strategy and inclusion criteria used for selecting relevant literature for the review. In terms of the SALSA (Search, Appraisal, Synthesis, and Analysis) framework [20], it is the *search* process where pre-specified eligibility criteria were not used in this study. However, in order to minimise the *publication and associated biases* that can be introduced due to this missing step in the search process, the study used a vast collection of papers and reports collected in the course of preparing past deliverable reports on CSA for the CyberSec4Europe project, particularly, D9.6 (performed systematic LR), D9.13 (performed systematic LR), D3.19 (performed non-systematic LR), D9.11 (performed field study and non-systematic LR), and D9.12 (performed non-systematic LR) (these deliverable reports can be found at [21]). Further, additional papers and reports on CSA and other domains were searched. In total, there were 703 papers and reports, which after the first round of manual screening were reduced to 129. The first round of screening was performed by reading the abstract, objectives, and surface reading (if needed) of the papers and reports. This was followed by a second round of screening and review done by reading each paper and report in detail. Both rounds of the review were performed to verify if the papers and reports discuss security attitude and behaviour change, or provide suggestions meaningful to the objectives set for this study. In total, 113 papers have been used for review and other purposes like making and justifying suggestions. The steps followed for the study are explained in Figure 1.

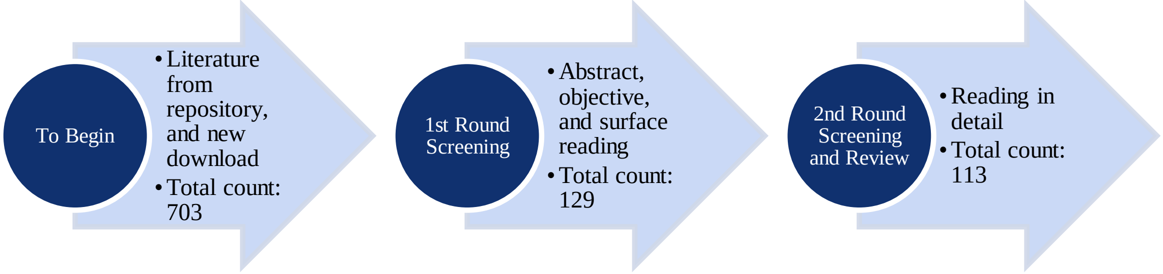
To Begin
Literature from repository, and new download
Total count: 703
1st Round Screening
Abstract, objective, and surface reading
Total count: 129
2nd Round Screening and Review
Reading in detail
Total count: 113

Figure 1: Steps of the research methodology

Identifying and eliciting the factors and properties for message framing and its effective delivery requires exploring a wide range of relevant disciplines to produce as inclusive results as possible. The non-systematic LR provided the needed flexibility to explore studies/works from both CSA and other relevant disciplines with insights and ideas useful for CSA purposes. However, there were a few challenges when adopting a non-systematic LR. The first one was to find adequate literature without being biased (originated from being selective about only a specific type of literature during the search process), which has been mitigated by incorporating the vast number of literature in our repository. The second challenge was the quality of papers selected for the literature. This has been mitigated by selecting only peer-reviewed journal and conference papers, and reports/white papers by organisations with a reputation for good cybersecurity research. In addition to flexibility, the methodology did not restrict from including relevant papers found during the review process. Last but not least, the methodology easily allowed the inclusion of gray literature (i.e., materials and research produced by all levels of government, academics, business, and industry in print and electronic formats, but are not controlled by commercial publishers, e.g., technical reports, dissertations and theses, white papers, conference papers, and patents [22]) in the review. Incorporating gray literature has several potential advantages, for instance, reduces publication bias, increases the review's comprehensiveness and timeliness, and fosters a balanced picture of the available evidence, thus enriching the review findings [22].

3 Review of Past Studies

This section reviews several related past studies. These studies come from various disciplines that can be beneficial for CSA. The review has been performed primarily to identify the relevant factors for effective CSA message framing and its delivery (or communication). The studies have been tentatively grouped under appropriate discipline.

3.1 Behavioural Theory

Among the various behavioural theories, notwithstanding the concept of behaviour is so broad that determining which theories may be labelled behavioural theories across different domains of academic research is problematic [23], the following four are the top investigated theories to understand security awareness and behaviour: Theory of Reasoned Action (TRA) (its extension Theory of Planned Behaviour (TPB)), General Deterrence Theory (GDT), Protection Motivation Theory (PMT), and Technology Acceptance Model (TAM) [24]. So, in this study, we focus on these four behavioural theories rather than delving into the specifics of too many of them. Moreover, a major limitation of many of these studies is that they mostly assess people's intentions for compliance and adoption of security behaviour rather than the actual security behaviour or compliance in actions. Indeed, the intention is a predictor of behaviour change however all intentions do not translate into actions (i.e., *intention-behaviour gap*) [25]; more specifically translate into the right actions to get the desired outcomes. Many unfavourable factors, for example, lack of adequate security knowledge, complex nature of policies, unusable security solutions, and priority of the individual's primary assignments (cause time and other resource constraints) negatively affect the course of intended behaviours. In addition to this, their suggestions are largely theoretical and do not elaborate on how these constructs can be applied in practice for security attitude and behaviour change. However, the limitations of past studies could be addressed to a great extent by investigating the actual behaviour of the participants (by using, for example, simulated attack-based tests) and the reasons for wrong security actions (by using, for example, a follow-up interview), preferably in the participants' natural environment.

In regard to these popular behavioural theories, firstly, Woo et al. [26] examined the significance of the PMT's constructs in influencing people's security decisions and behaviour. Their study revealed *perceived severity*, *response efficacy*, *self-efficacy*, and *response cost* to have a statistically significant effect on security decisions and behaviour. Perceived severity is a component of the *threat appraisal* and remaining (response efficacy, self-efficacy, and response costs) are components of the *coping appraisal*. Secondly, D'Arcy et al. [27] studied the impact of GDT's components on deterring employees from misusing Information Systems (IS). Their study found the *perceived severity of sanctions* to have a direct and negative effect on IS misuse intention. And it was also found to be more effective than the *certainty of sanctions*. Thirdly, Jones et al. [28] examined the effect of TAM's factors on employee acceptance of IS security measures. The result showed *subjective norms* moderated by management support have the strongest effect on the intention to use IS security measures. However, in contradiction to others and their own beliefs, they did not find any significant impact of *perceived usefulness* and *perceived ease of use* on the intention to use IS security measures. For this dissimilar finding, they alleged the poor message framing used in the study. Finally, Bulgurcu et al. [29] used an empirical study to demonstrate that employees' intention to comply with security policies is significantly influenced by the three constructs of TRA/TBP, attitude, normative beliefs, and self-efficacy. Further, they found out that both the *perceived benefit of compliance* (intrinsic benefit, safety, and rewards) and *perceived cost of non-compliance* (intrinsic cost, vulnerability, and sanctions) have a positive effect on employee's attitude toward security compliance, whereas the *perceived cost of compliance* (work impediment) has a negative effect on employee's attitude toward security compliance.

Interestingly, a systematic literature review performed by Mayer et al. [30] resulted in similar constructs from the aforementioned behavioural theories (except TRA) in addition to *perceived usefulness* and *perceived ease of use* to be useful for an information security context. Both *perceived usefulness* and *perceived ease of use* have a positive effect on security behaviour. Further, the study garnered the (negative and positive) effect size of each construct on information security; though its usability can be limited since the study does not furnish how the maximum effect can be acquired.

To sum up, these are the constructs that have a positive and negative effect on security behaviour, shown in Figure 2, and should be considered for CSA content design and delivery. The constructs that make a positive impact on security behaviour, i.e., encourage security behaviour and thus should be promoted in awareness initiatives are *perceived severity, response efficacy, self-efficacy, subjective norms, perceived benefits of compliance, perceived cost of non-compliance, perceived usefulness,* and *perceived ease of use*. Similarly, constructs that negatively affect security behaviour, i.e., discourage security behaviour and thus should be lowered in awareness initiatives are *response cost, perceived cost of compliance,* and *perceived severity of sanctions.*

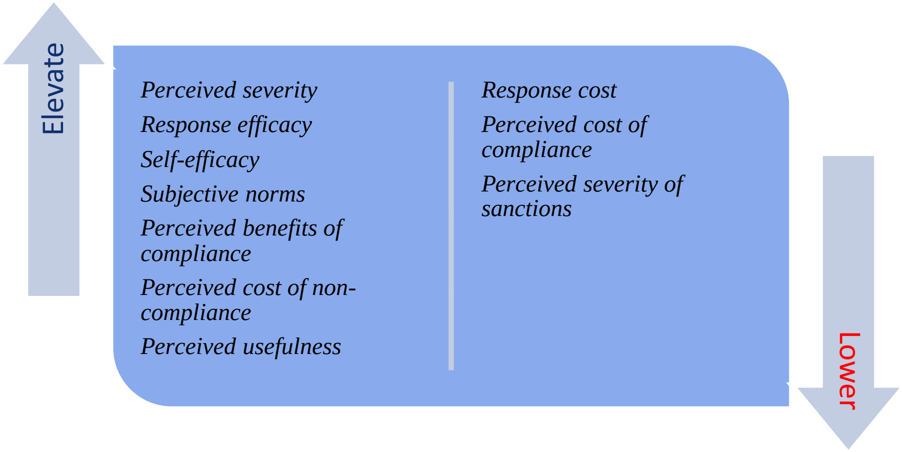
Elevate
Perceived severity
Response efficacy
Self-efficacy
Subjective norms
Perceived benefits of compliance
Perceived cost of non-compliance
Perceived usefulness
Response cost
Perceived cost of compliance
Perceived severity of sanctions
Lower

Figure 2: Constructs that have an effect on security behaviour

Some potential mechanisms to address these constructs are mentioned in Table 1. Certainly, applying these constructs is a necessary step to enhance the effectiveness of CSA but equally important are periodic monitoring and evaluation of security behaviour [31] and taking necessary interventions to address noncompliance and other unsafe behaviours that continue to exist.

Table 1: Constructs that affect cybersecurity behaviour and their potential mitigations

Behavioural Construct	Potential Mitigation
Perceived severity *(the magnitude of possible negative consequences a threat can cause if it succeeds* [30]*)*	• Explain and if possible demonstrate with real-life examples, how the threats could seriously harm [32] [33] in terms of, for example, loss of personal information, financial loss, embarrassment, discomfort, and disruption to functioning. But provide a realistic and convincing perspective (i.e., avoid assuaging or exaggerating the threat or being alarmist) [13] [34] otherwise it will lead to evidence being overlooked or could cause fear and anxiety in the audience. Although mild fear could be used to attract attention [35] and generate information-seeking behaviour [36], at an uncontrolled level fear is not healthy for security decisions.

Response efficacy *(the belief that a certain coping action will lead to the removal or at least a reduction of the threat* [30]*)* **Self-efficacy** *(an individual's perception of her or his own ability to successfully exhibit the recommended behaviour* [30]*)*	• People may not know about the available security measures. So, inform them about the prescribed security (technical and non-technical) measures and ways to access them. • Use pedagogic strategies like (refer to Section 3.4) ○ connect the learning with the audience's interests (for example, serious games for younger game lovers), ○ adopt collaborative and experiential learning, ○ start with simple tasks and gradually increase the tasks' complexity as the audience gain mastery of them. • Motivate communication with peers and instructors [37] [38] ○ provide credible communication and feedback channels, ○ encourage and create opportunities and time for communication. • Improve the computer competency of the audience so that they can implement technical security measures and apply security policies correctly.
Subjective norms *(the perceived behavioural expectations set by the individual's environment, in particular, close peers or people with higher authority* [30]*)*	• Clearly communicate the behaviours expected from the participants [13]. • Promote security behaviour as normal behaviour and social etiquette (*norms* in the MINDSPACE framework). • Utilise social proof techniques (social proof theory): ○ Inform about peers and people in authority whom others emulate and practice security behaviour by commending them publicly. ○ Use statistical data to demonstrate many others also practice security behaviour.
Perceived benefits of compliance *(intrinsic and extrinsic benefits that could gain by complying with security policies and performing coping behaviours* [29]*)*	• Make aware of the benefits associated with compliance [34] [39], e.g., intrinsic benefits, the safety of resources, and rewards.
Perceived cost of non-compliance *(intrinsic and extrinsic harms could cause due to noncompliance with security policies and avoiding/failing to execute coping behaviours* [29]*)* **Perceived severity of sanctions** (*the severity, i.e., magnitude of sanctions that follow an illicit act, e.g., violation of IS policy, abuse or misuse of IS resource* [30])	• Make aware of the harms a non-compliance could cause [39], e.g., intrinsic cost, the vulnerability of resources, and possible sanctions. • Make the individual aware of the prescribed security policies, and also the proportional sanctions and fines she endures for non-compliance with the security policies and misuse/abuse of IS resources [40] [41]. • Minimise the lucrativeness of non-compliance, for example, set multi-factor authentication to be the default, and if the user has to choose one-factor authentication, she has to work with the settings (change adoption choice from an opt-in to opt-out by default) [33].
Perceived usefulness *(an individual's subjective perception that using a specific system increases her or his effectiveness with regard to a specific task, e.g., solving an IS issue* [30]*)* **Perceived ease of use** *(an individual's subjective perception of whether using a specific system is free of effort, e.g., additional or complex steps that disrupt the existing workflow* [30]*)*	• Promote usable security (refer to D3.19 [31] and D3.5 [42]) to reduce the monetary expense, inconvenience, difficulty, and the side effects of performing the coping behaviour [43]. • Improve the computer competency of the audience so that they can implement technical security measures and apply security policies correctly.

Response cost (*all costs associated with performing the recommended coping behaviour or action* [30]*)* **Perceived cost of compliance** *(monetary and non-monetary costs that could incur by complying with security policies and performing coping behaviour* [29]*)*	• Promote usable security(refer to D3.19 [31] and D3.5 [42]) to reduce the monetary expense, inconvenience, difficulty, and the side effects of performing the coping behaviour [43]. • Provide intrinsic rewards [29] [44] (e.g., praising in public, asking for opinions on security-related decisions, providing positive feedback) whenever required. • Minimise the lucrativeness of non-compliance, for example, set multi-factor authentication to be the default, and if the user has to choose one-factor authentication, she has to work with the settings (change adoption choice from an opt-in to opt-out by default) [33].

3.2 Framing Theory

Knowing what information has to be communicated is important, but how it should be expressed or framed is far more important. People see and interpret the world through mental filters shaped by their personal beliefs, cultural influences, and individual characteristics [45]; this is a reason why people can come to a different conclusion or make a different choice despite having access to the same set of data or information [37]. However, their mental filters and decision-making can be influenced by the way a message has been framed or information presented to them. The way a message has been framed largely determines whether it will succeed in persuading people to perform a specific action or simply drive them away [46]; a well-crafted message has a high prospect of people understanding and responding to it rationally.

The same message can be framed in different ways that could evoke different emotions in the audience. For instance, a message promoting security policy compliance could be framed by emphasising the gains or benefits of compliance (i.e., incentives to motivate), emphasising the harms of non-compliance (i.e., loss or risk-aversion), or depicting a more balanced picture of both compliance and non-compliance. In addition to this, there can be considerable variation in the audience types [37]. Some individuals may take the risk more seriously if told how it could harm the group (e.g., the organisation or community they belong to), while others need to be told how it could harm them personally (e.g., identity theft, financial loss, etc.). Similarly, some people could grasp the idea of risk simply by its concept whereas other may require demonstration through the use of a suitable example to understand the risk.

Message framing, in general, is organising and structuring a message without altering the arguments or attributes of the featured product [47] by making it clear and effectives. It is built upon different *frames* (i.e., storylines aimed at making a problem relevant to a certain audience), and *framing effects* (i.e., occurs when a message frame is able to successfully alter the opinion of the audience on an issue). The two main functions of a message framing are *selection* (i.e., to select some bits of the information about the item being communicated) and *salience* (i.e., to make the information more prominent so as to support and promote the item being communicated) [48]. Although selection means deciding on what information to include, it also implies deciding on what information to exclude from the communication. Both inclusion and exclusion of information have a significant impact on the receivers' decision-making [49] [50]. In simple terms, exclusion means obscuring the information or alternatives from the message receivers, which could impact or alter their decisions or choices. Exclusion of information has high significance in communication for purposes like political campaigns and advertising where weaknesses are often concealed/removed. Even in the case of CSA, selecting only the information that needs to be known by the audience rather than the information that is good to be known is preferred. Providing too much or in-depth security information has a risk of causing confusion and cognitive overload in the audience, and thus may not result in the expected or desired outcome. Then, salience can be accomplished through different means, for instance, by strategically positioning the information, repeating the information, or linking the information with culturally known symbols. However, if the message comports with the existing schemata in a receiver's belief systems, then it may not require these means for saliency [48]. For example, an individual who has experienced and lost money to a phishing attack would understand its risks even when the information is not made salient. Not surprisingly, the same features to accomplish salience can be applicable in the case of CSA and are also in practice for the purpose, for example, conveying the same awareness message through different communication media like posters, emails, and games.

The impact of message framing on decisions has been demonstrated by some past studies, where a message framed differently produces different persuasive impacts, even the opposite, on the audience's decision-making, judgment, and responses both in general [47] [51] and CSA [34] communications. Thus, to craft a persuasive awareness message and deliver it effectively requires understanding how the human mind works and tapping its mental filters. In fact, several past studies have applied, for instance, social-behavioural and psychological, factors for message framing in order to improve the message's reception, interpretation, and absorption by the audience.

One such prominent study targeting message framing exclusively for awareness campaigns is by Bottomley et al. [36]. The study has listed various psychological factors that need to be considered when framing campaign messages. In general, a campaign message should be *clear*, *persuasive*, and *memorable*; however, these properties are achievable only if the message is framed with an understanding of human psychology. There are several biases, that emerge from heuristic-based decision-making and can be relevant to message framing. Some of these biases have been adapted for CSA message framing and presented in Table 2.

Table 2: Psychological factors for CSA message framing [36].

Psychological Factor	Potential Mitigation
Loss aversion (*People are more likely to be concerned by information on the losses of inaction than the gains obtained from the action.)*	The message should focus on the damages (or losses) to individuals, organisations, and society due to inaction or bad action. However, the losses should be immediate, connect to personal or professional life, and make sense (or has significance) to the audience.
Confirmation bias *(People tend to search for, interpret, favour, and recall information in a way that supports their prior beliefs or values.)*	Recognise the context when the message may not work and thus should come up with alternative messages with different offers depending on the audience.
Hyperbolic discounting *(People are less incentivised by rewards a long time in the future. They think of the future in a more abstract way.)*	The message should explain "*why is it important to know the threats*" for future threats (i.e., motivate them to be alert and stay safe), whereas for imminent events it should explain "*how to protect from the threats*" (i.e., prepare the audience to act) [13].
Affect heuristic *(Emotion has a wide range of effects on people's judgments and decisions.)*	The effectiveness of a CSA initiative can be significantly improved by altering the emotional appeal of the message. • The message should not focus on fear, uncertainty, and doubt (FUD) [11]. Positive emotions (e.g., prestige, hope) facilitate learning and memorability. • Negative emotions like fear-centric messages should be used to generate information-seeking behaviour (interest) and anger as a mobiliser to action; however, excessively negative emotions can backfire and discourage engagement.
Cognitive overload *(People cannot properly process information if it is more than what their working memory can hold or handle at one time.)*	• The message should contain only a sustainable amount of information that people can remember. • The message should present the information in a cognitively friendly manner. A memorable message has proven to lead to behaviour change. Memorability of a message can be improved by making the message unique and incorporating different cues or

	using media that support multiple cues (i.e., information richness to improve comprehension and retention of a message).
Bandwagon effect *(People align their support to things if shown others also do them.)*	The message should use statistics to further a position or prove a point (*Social proof theory*). But this has to be done carefully: use various measures to improve clarity (e.g., visualise data, frequency presentation), show the absolute value, and contextualise the statistical information (e.g., a big number does not make sense without a context).

Other similar studies made by de Bruijin & Janssen [34] and Furnell & Vasileious [3], dealt with cybersecurity message framing. The first study describes a strategy for cybersecurity message framing presented in Table 3. Whereas the latter briefly touched on how CSA contents should be designed and delivered and recommended *personalising* security message (i.e., a message should be framed and communicated directing specifically and appropriately at the target audience group rather than generically at everyone). Personalisation of security message is important to cover a diverse group of people who can receive it in the way that is most likely to lead each of them to a common vision [37], that is, the same interpretation and understanding of the message and with a similar level of persuasion. In order to personalise the message, factors like role, prior knowledge, barrier (e.g., personal and cultural values), learning style, security perception [3], and personality traits [17] [40] of the target audience group need be considered.

Table 3: Strategy for cybersecurity message framing

Strategy	Description
Do not exaggerate cybersecurity	Put the need for cybersecurity in a realistic perspective. Exaggerating the problem could be unproductive and lead to evidence being overlooked.
Make it clear who the villains are	Villains should be clearly recognisable as bad actors. Cast only unambiguous cybercriminals as villains.
Give the fight against cybersecurity a face: put the heroes in the spotlight	Those who are guarding and protecting should be placed at the forefront. They could be the cybersecurity specialists in the organisation. Explain the complex work they are undertaking to keep the systems safe and secure.
Connect cybersecurity to values other than security alone	The benefits of taking cybersecurity action should be emphasised. Cybersecurity is a benefit to economic growth and can provide a competitive advantage to the organisation.
Personalise for easy recognition	Connect cybersecurity to the daily life of people to ensure easy recognition.
Connect to other tangible and clear issues	Cybersecurity is closely interwoven with other issues that stimulate people much more than cybersecurity itself. These issues should be highly visible and have gained momentum, for example, terrorists using cybercrime to fund their activities.

Then, there are studies by Siponen [52] and Siponen & Kajava [2], which categorised the approaches to present awareness information into *prescriptive* and *descriptive* formats. The prescriptive format provides intrinsic action-guiding commitments to the objectives of awareness, whereas the descriptive format asserts some level of knowledge of cybersecurity and may not include such an action-guiding commitment to objectives. Among the five dimensions of information security awareness (i.e., organisational, general public, socio-political, computer ethical, and institutional education) [52], the descriptive format has been recommended over the prescriptive one for all except the organisational dimension. In the organisational dimension, security experts often want employees to internalise and follow the prescriptive guidelines. Both formats have their own limitations. Regarding the descriptive format, the awareness message could get misinterpreted and misused by the audience, and the audience may not have the ability to implement the message without action-guiding commitments. Similarly, in regard to the prescriptive format, without internalisation, binding and obliging the audience to follow guidelines could not be sustainable, and this could also raise ethical concerns, specifically the risk of indoctrination.

In addition to the factors identified by the aforementioned studies, it is also crucial for the awareness message to be *complete*. We believe that completeness should be an integral aspect of message framing, and this is where Entman's message-framing process [48] can help. If this message-framing process is adapted for CSA purposes, then a complete message should at least:

i) *state the problem*—what is the cybersecurity issue that the programme intends to cover;
ii) *assess and identify its causes*—what are the characteristics of the cybersecurity issue or attack that the audience can use to identify or detect it;
iii) *evaluate causal agents and their effects or impacts*—what are the harms that the audience may suffer if they fail to act or behave properly; and
iv) *recommend remedies*—what are the prevention or mitigation approaches that the audience is required to take.

Completeness in messages is important irrespective of communication types [53]. By completeness, it does not mean a lengthy text, but rather all information that needs to be known and if applicable to act properly. Studies like D9.13 [1] and D3.19 [31], revealed that several CSA materials do not have complete information. For example, many CSA posters are available with a one-liner slogan, which may succeed in catching the audience's attention but presumably, this will not help to achieve the ultimate objective of CSA, i.e., motivate to change security attitude and behaviour. Moreover, according to the Fogg Behaviour Model, three major components, i.e., Motivation, Ability, and Prompt (Nudge) [54] are important for behaviour change. This implies that to instigate each component, the awareness message should have some information or cues directed to it. Again, if we take into account our earlier recommendation for a complete message (i.e., considering Entman's message-framing process), then points *i-iv* are necessary for 'motivation', points *ii & iv* predominantly develop 'ability', and point *iii* acts as 'nudge'.

Interestingly, a survey conducted by Arain et al. [32] with healthcare workers to measure the effectiveness of their existing IT security and privacy education and awareness modules resulted in suggestions on content improvement similar to Entman's message-framing process. The participants suggested including information on:

- how to recognise the threat,
- how severe the threat and its consequences are, and
- how to apply the appropriate measures or achieve security behaviours or respond to security breaches.

Also, ENISA [13] has similar recommendations for a CSA message. It suggested a CSA message, in its simplest form, to have at least:

- a statement of the risks and threats,
- why it is relevant for the audience to know about them,
- what the audience needs to do and not to do, and finally
- how to protect from the threats.

Positiveness in message phrasing and framing is another important factor. A positively phrased and framed message has been found to be more persuasive (in terms of how the audience process and respond to the message) compared to a negatively framed message essentially when there is little emphasis on detailed processing [55] [56]. So, in the case of CSA where the knowledge disseminated is not in-depth and ideally has no active involvement of the audience [57], positive framing of the message presumably could be more persuasive [17]. A positive message can be used in suggesting measures, for example, a recommendation "*do not use a weak password*" can have a positive alternative as "*always use a strong password*." The first option tells what not to do and uses negative words whereas the second option tells what to do and uses positive words. Moreover, the need for positiveness becomes more crucial when presenting factors like factual information and expectations in order to enforce or motivate the audience to decide and act rational, i.e., between "*glass half full*" and "*glass half empty*" situations, where the optimistic view of "*half full*" is preferred for reporting [57]. For example, a preferable option for the statement "*the organisation targets to reach 20% noncompliance of GDPR*" could be "*the organisation targets to meet 80% compliance of GDPR*."

A *compelling* message with concrete calls for achievable actions has been another factor suggested by Christiano & Neimand [14]. Their main argument for this is that without calls of action, the message will simply contribute to probably knowledge gain and nothing more.

Moreover, every included information cannot be of the same priority, for instance, among the different characteristics for identifying a phishing attack, some are more precise than others. In such a case, the most important information should be placed at the beginning and end of a series of information. This is important to mitigate the effect of *serial position effect* (i.e., people remember primary information or primacy effect and recent information or recency effect) [58].

Finally, simplicity or clarity in the language used to compose the message is very important. Using familiar vocabulary enhances the *comprehensibility* and *memorability* of the message [59].

To sum up, the various suggestions compiled from these studies for an effective CSA message framing (i.e., content design) are:

- *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 descriptive format for the message presentation, except for the organisational awareness where 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.*

3.3 Communication Theory

Communication is much more than a mere exchange of information. It also includes understanding the meaning of the message conveyed and its underlying intentions. So, conveying the right message is complex as the meaning of the message could easily get misheard, ignored, perceived irrelevant, misunderstood, or misinterpreted if it is not effectively communicated. In general, the topic '*communication*' has been widely studied for many years. These studies pertaining to communication with the purpose to address the communication needs and concerns in different fields have resulted in several models, theories, and frameworks. Some communication models/ theories/ frameworks that we believe have validity in CSA and also observed in many studies on CSA conforming to their recommendations are mentioned next.

The Lasswell Model of Communication [60] provides five components or *Ws* that need to be addressed in all effective communication, which are:

- *who* (source of the message)—someone with authority, expertise, and trust*;*
- *say what* (content of the message)—correct and unbiased message*;*
- *in what channel* (medium)—best-fit medium;
- *to whom* (receiver of the message)—audience grouped based on demography, behaviour, or job; and
- *with what effect* (the desired effect)—message impact and audience feedback.

Similarly, the 7Cs [53] of effective (oral or verbal) communication widely popular in business and management communication are:

- *completeness*—the message contains everything that the audience needs to be informed about and, if applicable, act;
- *conciseness*— the message is brief, to the point, and comprehensible;
- *consideration*—the message considers the audience's viewpoints, requirements, problems, background, mindset, education level, etc.;
- *clarity*—the message is easy to understand, i.e., considers the specific goal, and has exact, appropriate and concrete wordings;
- *concreteness* —the message is clear and particular;
- *courtesy*—the message is unbiased and does not hurt anyone's feelings; and
- *correctness*—the message is correct in language and facts and is well-timed (at what time the message is communicated has a critical impact on its reception).

The next model is Monroe's Motivated Sequence [61], which can be utilised to create and arrange the components of a complete message. Its five principles of speech are based on the psychology of persuasion, which are:

- *get attention* — establish credibility and authority, and state the purpose or audience to expect;
- *establish the need*— convince the audience there is a problem, use statistics (or examples), inform about the consequences of maintaining the status quo, and how the problems can affect the audience;
- *satisfy the need*— introduce solutions, discuss facts, and clearly state what you want the audience to do or believe;
- *visualise the future*— visualise the situation if nothing is done (use positive method, negative method, contrast method to persuade; and
- *action/actualisation*— leave the audience with concrete actions they may take to resolve the issue.

Similar to other fields, effective communication is crucial in CSA [62] [63] and this is where the components or elements of communication models and theories could play significant roles. In fact, we clearly see some of these suggestions have been utilised for the communication of cybersecurity issues in the forthcoming sections. For example, '*messenger*' of the MINDSPACE framework (discussed in Section 3.5.1) has similar recommendations as '*who'* of the Lasswell Model of Communication. In order to apply these suggestions, however, sometimes it may require adapting their meaning and implementation approach to make sense and best fit for cybersecurity purposes. For instance, for CSA purposes, a trustworthy messenger would be someone who is a qualified professional or certified practitioner possessing relevant degrees or certifications.

Apart from these communication models and frameworks, there are studies that have investigated the communication challenges in CSA. Bottomley et al. [36] recommended factors for an effective message delivery, which are presented in Table 4.

Table 4: Factors for awareness message delivery

Factor	Potential Fostering Mechanism
Targeted message	The message should target a specific audience group. Group can be based on opinions or pre-existing beliefs on cybersecurity held by the audience, cybersecurity expertise of the audience, or demographic information. However, pre-existing beliefs and cybersecurity expertise make better criteria for grouping.
Effective medium for message delivery	Each delivery medium has its own pros and cons that make it suitable for a certain situation. Similarly, the audience group can have their preference for a particular medium over others. The selected medium should best fit the content type that would be communicated and also preferred by the audience (i.e., the audience knows how to use it and enjoys using it).
Appropriate messenger	The messenger influences how rapidly the message will be spread and also how seriously it will be taken. Someone who is trustworthy and liked by the audience can be a suitable messenger.
Building coalitions	Coalitions can create a broader pool of resources and expand reach so they should be utilised for CSA message communication. However, for a coalition to be successful, it needs the ability to: lead and organise its stakeholders, adapt to changes, manage resources efficiently, and have the technical capacity to implement the necessary functions.

Chipperfield & Furnell [37] provided the benefits and suitability of the two types of communication, i.e., *vertical (or downwards)* and *horizontal (sideways) communication*, classified based on the direction of hierarchy within an organisation. The same communication types are used for communicating CSA information in an organisation.

- In *vertical communication*, information is passed from superior to subordinates and it is less of a two-way process. It can be suitable for communicating the aspects of security that are critical and integral to core business operations (and so leave limited room for debate or discussion). Nevertheless, integrating ways to communicate suggestions for improvement upward would make the communication more relevant to them.
- *Horizontal communication* occurs at the same hierarchical level between colleagues or peers. It is often informal and more of a two-way process between individuals with perceived equality between the roles and trust for each other. This has a potential to communicate general concepts or advice on a security issue if properly applied.

House & Giordano [64] studied the impact of (im)politeness in security communication. Their study did not find any significant difference in intention to comply with security directives between polite and impolite text and image-based messaging; however, they found a significant difference between polite and impolite in video-based messaging. The polite message performed better than the impolite message in video-based messaging. We believe that, regardless of the message type, there should be politeness in the awareness message.

Shaw et al. [65] tested the impact of information richness [66] on the information security awareness level. In order to do so, they used three media, i.e., hypermedia, multimedia, and hypertext with different information richness, and measured the awareness levels using three levels, which are: *perception* (understand the presence or awareness of a threat), *comprehension* (comprehend, understand, and assess the danger posed by different security risks), and *projection* (ability to project or predict the future course of security attacks). The main findings are:

- *Hypertext-based instruction* is effective in improving users' perceptions of security risks.
- In terms of comprehension and projection, *multimedia-based instruction* surpassed *hypertext-based instruction*.
- When used correctly, *hypermedia-based instruction* is suitable for perception, comprehension, and projection.

The study further revealed that information rich media (containing both verbal and non-verbal cues) and features for feedback are found to be more effective in the communication of awareness messages.

To sum up, among the various components of communication theories, the following could be relevant for CSA message communication:

- *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 strategy could be targeted to a specific audience group;*
- *ensure the content of the message is factually correct, clear and concise, lacks bias and uses courteous and polite language*
- *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 part 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; and*
- *use delivery channels that are suitable for the content being communicated, the target audience group (the channels should best fit the content, and the audience should feel comfortable and preferable to use them) and have high information richness and feedback features.*

3.4 Pedagogical Approach

Pedagogy refers to the method and practices used for teaching and learning and is impacted by and takes into consideration the social, political, and psychological development of learners. There exist many models, frameworks, and paradigms of pedagogy in theory and practice. No doubt, CSA also encompasses the different components of pedagogy, such as *psychological context* (motivation, persuasion, and enforcement of CSA), *curriculum development* (CSA content design), *teaching methodology* (delivery or dissemination methods for CSA), and *evaluation of learning* (CSA effectiveness evaluation), though they may not be as intensive and distinct as in security education and training [67]. This also means some recommendations from the existing pedagogical approaches can be helpful in designing appropriate paradigms for CSA purpose and context. In spite of that, barely any study has attempted to explore CSA from a pedagogy perspective. Obviously, there are several studies analysing the different pedagogical strategies for cybersecurity education and training purposes. Interestingly, most of them have emphasised the use of *experiential learning* through, for example, in-class laboratory exercises [68], simulation exercises [69], and serious games [70], for cybersecurity education and training.

An interesting and important study that scrutinised the paradigms of learning for security training in a more holistic way is by Karjalainen & Siponen [71]. This study provided pedagogical requirements for information security training, which coincide with the aforementioned studies and emphasised *experiential and collaborative learning*. Some requirements put forward by them that could also be relevant for CSA purposes are as follows:

- *Psychological context*— Due to the nature of cybersecurity, it requires communal effort and change, for example, it is a shared responsibility of every employee in an organisation to protect it from cyberattacks. Therefore, the learning paradigm should be based upon a *group-oriented approach* (where learners discuss, interact, share information, and provide feedback on the topic) to teaching and learning.
- *Content*—The content should be based on the *learners' collective experiences and meaning perspectives* to make it community- centred, understood, accepted, and implemented collectively.
- *Teaching method*— The teaching methods should focus on *collaborative learning* in order to reveal and produce collective knowledge.
- *Evaluation of learning*—The evaluation should emphasise *experiential and communication-based methods* from the viewpoint of the learning community.

Thomson & von Solms [72] recommended *instrumental learning* (learning through reinforcement) and *social learning* (learning through observation) along with the implementation of various persuasion techniques, namely, conformity, obedience, reciprocity, and commitment (these persuasion techniques have been discussed in Section 3.5.1) for cybersecurity education and awareness. They posit that using these learning and persuasion techniques can contribute to persuading people to behave in a certain manner, regardless of their attitude towards the subject, their knowledge about the subject, or their emotional feeling about the subject. In instrumental learning, the study suggested using two techniques, *operant learning* (praise for correct behaviour and reprimand for incorrect one, i.e., learning through reinforcement), and *shaping* (begin with simple and gradually increase the standard as the individual's abilities improve). Similarly, in *social learning*, people learn by observing and imitating the behaviour of others. It has the following mediational processes that help to determine whether or not a new behaviour is acquired:

- *exposure and attention* —in order to persuade someone of something, they should first listen and give closer attention to the message (make it mandatory to attend a CSA program and emphasise how the information is useful and new),
- *comprehension*—should understand the message otherwise there will be no worth of exposure and attention (use printed media to convey complex messages and broadcast media to convey simple messages),
- *acceptance*—should accept the message otherwise there will be no worth of understanding (use high quality and well-scrutinised information in the message), and
- *retention*—developed attitudes should retain for a significant length of time (repeat the important facts or information).

Yoo et al. [38] pointed out two main factors, *flow* (i.e., completely immersed in the activity), and psychological *ownership* (i.e., the feeling of possession over a target) to motivate people to learn or influence security education, training, and awareness (SETA) and practice (compliance) security. And in order to achieve these factors, they suggested to:

- Use materials that *suit the audience's current knowledge and skill levels*.

- Provide *positive feedback* (in the forms of rewards, awards, and messages) to report the audience's progress and acknowledge their achievements.
- Give *autonomy* to the audience, for example, on how, when, and where they want to learn about security.
- Make the *learning experience entertaining* so that the audience can feel like investing their precious time and energy. But ensure that entertainment does not dilute the real purpose of awareness.
- Incorporate *social interaction* (for example, with colleagues and peers) and technologies (or channels) to facilitate and make this possible.

Vasileiou & Furnell [73] proposed a framework for personalised SETA. Their framework was based on the *threshold concepts* and demands integrating the concepts and deeper understanding of security the learners need to acquire and develop their ideas. To begin with, the framework suggested collecting information about the learners, namely role, prior knowledge, barriers, learning style, and security perception, using a questionnaire so that their position in relation to the threshold concepts could be understood. Next, it suggested tailoring the security learning experience based on the information and using the learning content and delivery medium that best fit the learner's learning style. Finally, it is suggested to incorporate peer-based support to further reinforce and enhance the learning and acceptance of security by the learners.

Arain et al. [32] suggested providing relevant and role-specific examples, up-to-date content, short modules, flexible learning modes, multiple delivery methods, and a grading system for an evaluation in order to improve the effectiveness of security awareness programmes.

Siponen & Kajava [2] described the user acceptance and internalisation of security awareness as gradual processes and long-term goals. This means people can be at different stages of attitudinal change, naming a few stages on the progress wards (positive) could be readjustment, cooperation, acceptance, and internalisation; whereas regression downwards (negative) stages could be repulsiveness or hate. Thus, they suggested measuring the level of people's attitudes to understand the different types of security behaviour one can expect and encounter. Further, they proposed to use the adapted version of the persuasion method by Stevenson [74] in addition to the occasional use of rewards and sanctions in security education and awareness, particularly in motivating people to make positive transformations in their security attitude and behaviour. Some potential approaches they recommended to influence people's attitudes and behaviour change are:

- *logic*—all prescribed security actions should be logical,
- *emotion*—security measures should provoke appeal to emotions in a positive manner,
- *morals and ethics*—security norms should be based on moral and ethical principles, at least those imposed by legislation,
- *well beings*—should show how lax security measures could jeopardise the well-being of individuals, organisations, and societies,
- *feeling of security*—should give the impression of safety by adhering to security procedures,
- *rationality*—should provide rational explanations for security guidelines, procedures, actions, or behaviours.

Currently, CSA has widely been investigated from the perspective of effective delivery of relevant security information to the target audience and enforcing/motivating them to adopt it. However, a major shortcoming of this approach is that it rarely considers the fact that the target audience could have pre-existing assumptions, conceptions, and misconceptions as a result of incorrect thinking, flawed misunderstanding, or belief based on incorrect information about the security issues [75] [76] [77] that must also be addressed (modified, refined, or omitted) by the CSA initiatives for a sustainable behaviour change. Otherwise, this prior conception could conflict and interfere with the newly delivered conceptions and could result in *cognitive dissonance*—discomfort resulting from holding two conflicting ideas simultaneously—in the audience. Some implications of this could be, for example, the audience encounter difficulty in understanding and grasping the new knowledge, the audience is uninterested in learning and adopting the new knowledge [78], and more importantly, the chance of *regression* of old security behaviour is high among the audience who do not have fundamentally understand the security concept [77]. The relevance of this aspect in CSA may be felt more in the current time, essentially, when people are consciously and unconsciously absorbing much disinformation and misinformation (including on cybersecurity) from the Internet and other media every day.

In order to deal with a situation where the new knowledge is relatively advanced or deviates too much from the learners' existing conceptions and requires a conceptual change in the learners, Chan & Wei [77] [79] validated and suggested implementing *constructivist pedagogies* or *constructivism* that consider the learners' epistemological beliefs and required a level of learners' active participation rather than being a passive recipient of information. In general, constructivism consists of four critical components, which are: elicitation of prior knowledge or preconception, creation of *cognitive dissonance* to challenge preconception, applying new knowledge with feedback or conceptual restructuring, and reflection or assessment on learning [80]. Similarly, serious games [31] and online tools [1] are gaining popularity for CSA purposes that also require the active participation of the audience. These approaches are in agreement with Dale's Cone of Experience for instructional design and learning processes, which proposed that learners retain more information based on what they "*do*" (through hands-on learning or active learning) rather than what they "*hear*", "*read*" or "*observe*" [81].

To sum up, the following learning approaches should be utilised to improve the effectiveness of CSA initiatives:

- *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 progress in multiple stages, and use persuasion techniques (logic, emotion, moral and ethics, well-beings, 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., uses media suitable for the learners, includes feedback interventions, provides autonomy in learning processes/flexible learning modes, is entertaining to learn, involves social interactions, provides role-specific and relevant examples, uses up-to-date content, uses short and comprehensible modules, and implements multi-delivery methods).*

3.5 Social Psychology and Behavioural Economics

Daniel Kahneman in his book "*Thinking Fast and Slow*" [82], has split human thinking and reasoning into two systems. *System1* is unconscious, automatic, and quick but error prone whereas *System2* is deliberate, conscious, and reliable but slow and effortful. In an awake individual, both Systems 1 and 2 are active, however, at varying intensities. A vast majority of everyday thinking is done by System1 which continuously generates suggestions for System2. If the suggestions are endorsed by System2, which happens most of the time with little or no modification to them, then the suggestions may translate into actions. It is only when System1 runs into difficulty that System2 is called for more specific and detailed processing of information in an attempt to solve the problem.

The shortcuts that System1 makes are *heuristic*, i.e., the knowledge structures, presumably learned and stored in memory [83]. But the heuristic processing is constrained by the basic principles of knowledge activation and use, namely, *availability* (knowledge being stored in memory for future use), *accessibility* (ability to retrieve the available knowledge in memory for use), and *applicability* (relevancy of the retrieved knowledge to the decision task) [84]. Thus, the heuristic is built by reviewing the limited information at hand (since all relevant information cannot be recalled, and all recalled information cannot be salient to the problem) and connecting that information to past experiences with similar problems. This also means that heuristics can be wrong and biased.

Naturally, people are influenced by cognitive and cultural biases, and susceptible to persuasion techniques. These impact their experience, decision-making, and behaviour, including those conflicting with intentions and beliefs. With no complete escape from these biases, it is suggested to be aware of them and stay prepared. Awareness of these biases will enable us to acknowledge the weaknesses in our thinking and reasoning, and probably also get motivated to self-regulate and self-reflect on our thinking and reasoning. Moreover, it will guide us to avoid the contexts/ situations/ events/ things, whenever possible, that may contribute to instigating and shaping biases. Similarly, understanding and applying the persuasion techniques, also often used by cybercriminals to conduct their malicious acts (for example, conducting phishing and social engineering attacks) [85], can be helpful in persuading people to adopt security behaviour.

In CSA, many persuasion techniques, and technical measures can be applied to minimise the effect or errors caused by cognitive and cultural biases in security decision-making and actions. Several past studies have investigated this dimension of cybersecurity and looked into social psychological and behavioural economics factors that may require to be addressed and sometimes utilised to design more effective CSA initiatives that encourage System2 thinking. Essentially, in cyberspace that is dominated by speed, and slowing down is often considered an inconvenience [33] (also a reason why System1 thinking has become standard), promoting and preparing for System2 thinking in cybersecurity is of utmost importance.

However, all irrational decisions may be biased rather than intentional. The *concept of bounded rationality* [86] explained why seemingly logical people sometimes make apparently irrational security decisions, as perceived by an independent observer. It identified mainly four reasons that limit the individual from making optimal security decisions:

- People make decisions based on their *existing beliefs and attitudes*, and each person has their own set of experiences as well as an endless range of beliefs and attitudes. As a result, some people see information security management as beneficial, while others see it as a hindrance.
- People make decisions depending on their own *perceived cognitive limitations* when faced with technological complexity and a poor user interface.
- People make decisions based on *time and resource restrictions* while keeping other activities and objectives in mind. Competing inputs and time restrictions are likely to enhance the chance of people using "rules of thumb" or heuristics to make decisions. While rules of thumb and heuristics

are useful and usually produce a reasonable result for the individual, they are unlikely to produce an optimal result.

- People learn to be satisfied with a *satisfactory result* rather than an ideal one. Excessive resource investment in optimising one option might result in fewer resources available for subsequent decisions. This constraint leads to a search for acceptable rather than optimum solutions.

3.5.1 Persuasion Principle

Persuasion is the process of influencing or convincing others to change their attitudes or behaviours by using rational and/or emotional arguments. There are different persuasion strategies in practice. Some of them, which we have found to be utilised for CSA purposes are discussed next.

An early and simple approach for persuasion suggested providing *plausible arguments or reasons*. This applies even if the arguments are vacuous, an exception being a thoughtful persuasion where the arguments have to be true. Overall they should preferably demonstrate how listeners can benefit from changing their attitudes [87] [35]. However, a more holistic and complete view of the persuasion approach has been given by the Yale Communication Model [35], which posited the following four interacting factors to create a persuasive effect: "*who*— communicator", "*what*—organisation, and content of the persuasive message", "*whom*— the audience", and "*means*— communication channel or medium" (i.e., the first four components of Lasswell Model of Communication). These factors provide input into three mediators of persuasion: *attention*, *comprehension*, and *acceptance* (in other words, persuasion occurs when the target audience pays attention to the message, then comprehends or understands the message's content, and finally accepts the message's content). In order to create a persuasive effect, there are various variables that can influence each factor, for example:

- *communicator*— attractiveness and authority (power) are important variables; however, credibility (trustworthiness and expertise) is the most important variable for persuasion;
- *message*—evoke low (or enough) fear to grab attention but also require providing possible solutions;
- *target audience*—present messages tailored to different audiences. For example, determine the suitability of rational arguments versus emotional arguments for different audience; and
- *communication channel*— as above, determine the suitability of using two-way versus one-way communication depending on the audience.

Another equally important work is by Robert Cialdini [88], who provided the highly popular six principles of persuasion in his book "*Influence: The Psychology of Persuasion*". These principles were originally designed to explain how people make decisions in relation to sales and purchasing, but now have been widely adopted in other fields of study, including cybersecurity. In cybersecurity, these principles can be effective tools to persuade people to change attitudes toward cybersecurity and motivate them to practice safe and secure behaviour in cyberspace. These six principles are as follows:

- *reciprocation*—a tendency to give something in return;
- *commitment and consistency*— a likelihood to stick to a cause or idea after making a promise or agreement (consistent with identity or sense of self-image);
- *social proof*—a tendency to imitate the behaviour of other people (conform to the norms of a social group);
- *liking*: a tendency to like someone who is similar in terms of interests, attitudes, and beliefs;
- *authority*—a tendency to obey the request of figures who are authoritative, credible, and knowledgeable experts; and
- *scarcity*—a tendency to acquire a product, service, or information that has limited availability.

Some studies that utilise the concepts of human behaviour and psychology to make distinct recommendations for motivation purposes exclusively in CSA are by Bada et al. [6] and Coventry et al. [89], which suggest utilising the *MINDSPACE framework* [44] to deliver cybersecurity best practices. The MINDSPACE framework captures nine non-coercive influencers for behaviour change. These influencers are based on different established psychological and communication theories. Although the framework has been initially designed for public policies aiming to change or shape people's behaviour, it can also be adapted for CSA purposes. Table 5 provides the nine influencers of the MINDSPACE framework, psychological and communication theories each influence is roughly based on, and potential ways to apply them to influence people's cybersecurity behaviour.

Table 5: Application of MINDSPACE influencers in CSA

Influencer	Mitigation Mechanism
Messenger *(People are heavily influenced by who communicates information.)*	• The source of awareness information should be someone (person or organisation) to whom the audience is most likely to listen, e.g., someone with authority, someone with similar characteristics, or someone whom others trust and like. • The appropriate messenger could be a security expert, trained executive or close peers (whom the participants like and trust), or an organisation authorised for cybersecurity.
Incentives *(People's responses to incentives are shaped by predictable mental shortcuts such as magnitude and time of incentives, and strongly avoiding losses.)*	• The incentives (negative or positive) referred should be intrinsic, immediate, and are linked to something that makes sense and matters to the participants. • The emphasis should be given to the losses that the audience or their organisations may suffer if failed to behave securely, or the security fails.
Norms *(People are strongly influenced by what others do.)*	• Good security behaviours should be repeatedly promoted as social etiquette and normal behaviour (e.g., executives can set up an example by always locking their computer before leaving it unattended). • The promoted behaviours should be the target audience as much as possible. • Let the audience know who else (someone whom the audience may emulate, such as colleagues, executives, or leaders) practice security behaviours by commending them publicly.
Defaults *(People "go with the flow" of pre-set options.)*	• The security choices that reflect the organisation's norms and regulations should be preselected by default, for example, security software should be installed and be part of the initial setup. In other words, secure or right choices should be simple and smooth to perform whereas risky behaviours are discouraged by making them difficult to perform.
Salience *(People's attention is drawn to what is novel and seems relevant to them.)*	• Security information and images that the audience can understand and relate to personal lives/experiences should be used. • Communication should be kept simple (simplicity and clarity in language, cognitively friendly amount/type of information), personalised, and accessible.
Priming *(People's acts are often influenced by subconscious cues.)*	• The audience should be frequently exposed to messages or cues that remind of and influence security actions, for example, security posters on the organisation premise and screensavers on employees' computers.
Affect *(People's emotional associations can powerfully shape their actions.)*	• The audience should be informed about the purpose of the CSA programme and their role in preventing security attacks. • Provide awareness materials that are relevant (understandable and accessible) to the participants.

	• Present security message in counterintuitive manners so that it provokes emotions (attitudes to cybersecurity) but without obviously connecting it to a change in security behaviour.
Commitments *(People seek to be consistent with their public promises and reciprocal acts.)*	• The programme should have clear goals and expectations concerning the desired behavioural changes following a CSA programme and they should be made public (known to the audience). • If possible, a deadline should be set by when the goals have to be achieved. Incentives should be offered for good security behaviour (reciprocity).
Ego *(People act in ways that make them feel better about themselves.)*	• The capabilities and motivation of the audience should be considered and possibly begin with small and easy changes. • The audience should receive structured and constructive feedback on their behaviours (performance).

Further to complement the MINDSPACE framework, the Behaviour Insights Team [41] developed the EAST framework, which will be discussed in Section 3.5.2.

Persuasion, in general, can occur at all levels of *mindfulness*, which can be *thoughtful persuasion* (when a listener is motivated and weighs the pros and cons of the provided evidence before making the transformation in attitudes and behaviour) or its contrasting *mindless persuasion* (when a listener lacks motivation and uses little intellectual analysis in contemplating the provided evidence before making the transformation in attitudes and behaviour) and everywhere in between [87] [90]. In a real-life, many social influence variables operate under conditions of mindlessness [87]. The same has been evident from the Langer et al.'s experiment [91] that revealed both oral and written communications, whether *semantically sound* or *senseless*, are vulnerable to *mindless behaviour* (i.e., the listener pays no attention to the substantive information relevant to resolving the problem successfully, or pays attention to a small amount of structural information that may not be useful). Further, it demonstrated that the ignorance of relevant information will continue to occur unless the communication occasioned an *effortful response* or is *structurally novel*. However, the study also pointed out that the tendency to ignore relevant information may not always be completely mindless, and could have occurred simply due to, for example, the listener knows the information, the information is congruent with his/her past experiences, s/he believes the information to be irrelevant, or s/he has found structural cues to proceed.

Finally, it is important to understand that persuasive tactics applicable in an audience group may not work on others, so these tactics must be tailored to fit the audience group in order to change attitudes [92]. The persuasive tactics can be impacted by variables like personality traits of the audience (refer to [93] for the relationship between personality- Big-5, Dark Triad, and Type D and susceptibility to Cialdini's six principles of persuasion), personal relevance of ideas to the audience (a high personal relevance is governed by a thoughtful persuasion whereas a low personal relevance is governed by a mindless persuasion) [94], and the audience's pre-existing attitudes or attitude accessibility (a weak attitude encourages a mindless persuasion and is more susceptible to change in response to persuasive appeals whereas a strong attitude encourages a thoughtful persuasion and requires strong arguments for persuasion) [95].

To sum up, persuasion techniques relevant to CSA and can be utilised for the purpose are:

- *provide plausible arguments on how the audience benefits by changing security attitudes or behaviour, use attention-grabbing message (entertaining content or raising mild fear may work),*

- *use a credible (trustworthy and expert) communicator, and messages and communication channels tailored 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; and*
- *provide structurally organised content and enforce effortful response.*

3.5.2 Nudge Theory

In behavioural economics, a '*nudge'* is a way to manipulate people's choices to lead them to make specific decisions. Studies by Bavel & Rodriguez-Priego [96] for the European Commission, Bavel et al. [97], and Sharma et al. [98] implemented the "*Nudge theory*" for security behaviour change.

The first study [96] explored and tested the role of nudges (i.e., features of the environment that attract attention and indirectly encourage to alter behaviour) on online decision-making, particularly in cybersecurity. The study demonstrated that utilising the *nudge theory* can be effective in generating more secure behaviour. A CSA programme generally presents, for example, what to do, why to do it, ways of doing it, and so forth but often this knowledge does not translate into actions. By introducing suitable cyber nudges, such a situation of inactions can be minimised. Appropriate cyber nudges will act as soft enforcement, which will drive and steer the audience to use the learned security practices [99]. However, the challenge of using this technique is finding the right "*nudge*", which can quickly become complex. For example, Bavel & Rodriguez-Priego used nudges based on established concepts like PMT (e.g., heightened coping appraisal, heightened threat appraisal, and combined coping and threat appraisal); gain versus loss framing (e.g., gain-framed warning message, and loss-framed warning message); anthropomorphic characters (e.g., female anthropomorphic character, and male anthropomorphic character); and low-risk, high-impact versus high-risk, low-impact (e.g., high-risk, low-impact condition, and low-risk, high impact condition). Interestingly, these cyber nudges produce a varying effect on the audience for different security behavioural measures. First, among the PMT appraisals, heightened *coping appraisal* was found to be the most effective for behaviour change, i.e., people fail to behave securely because they do not know what secure behaviour entails. The other two appraisals were found relatively less effective. Second, regarding the gain versus loss framing, both messages were found to have a positive effect on the security behaviour change. Finally, among male and female anthropomorphic characters, the *male character* was found to be effective but only in one security behavioural measure.

The second study [97], from the same author group, used an experiment to test the impact of PMT's constructs, mainly *coping message* (information on how to minimise exposure to risk), *threat or fear appeal* (highlight the potential negative consequences of not acting safely), and both messages combined (i.e., coping message and threat appeal) in triggering or nudging online security behaviour. Further, the study analysed the impact of age and national culture on online security behaviour. It revealed that *coping messages* and *combined messages* have an effect on security behaviour change, whereas threat appeal has not. Likewise, both age and country have a significant effect on online security behaviour.

Finally, the third study [98] that was recently conducted to test the impact of nudging in the context of CSA. They used an experiment to examine the impact of framing and priming (*digital nudging*) on people's security behaviour. In conformity with past studies, they found that priming (conducted by using instance-based information on potential security risks to prime tech-savvy young adults) plays an important role in security behaviour; it encourages people to make safer and more secure actions. However, although strange, the study did not find any significant role of message framing (whether it is negative or positive) in cybersecurity behaviour. As a rationale for the latter finding, the study admits that this could have happened possibly due to the weaknesses in their message framing, which were generic and perhaps had no new information to offer to the tech-savvy young participants.

While implementing the "*nudge theory*" for security behaviour change, one of the major challenges is determining suitable nudges. All the above-mentioned studies are dependent on nudging techniques that are particularly restricted to *message framing*. Along with message framing, many other aspects can be used for nudging, for example, a report by Suter et al. [99] from DayBlink Consulting, utilises behavioural science concepts (mainly *cognitive biases*) to generate cyber nudges with the objective of bringing sustainable security behaviour changes in people. Some cyber nudges suggested, by the study are listed in Table 6. These suggested cyber nudges are largely associated with usable security.

Table 6: Cyber nudges for security behaviour

Cognitive Bias	Rationale	Suggested Cyber Nudge
Affect heuristic and risk assessments	Affect based evaluations are quick, automatic, and rooted in visceral emotional reactions rather than calculated judgment. They are more pronounced in resource constraint situations (i.e., when lacking resources or time to reflect on risks and benefits).	• Use security pop-ups and warnings with messages that remind users about security risks and make their potential consequences/costs more salient.
Habituation and security warnings	People exposed to a similar stimulus (or similarly designed warning message) often get desensitised to it and are more likely to ignore security notifications and warnings (or encourage automatic click-through).	• Use pop-ups and warnings only when necessary. • Use pop-ups and warnings with unfamiliar user-interface features, for example, polymorphic, or colour-changing warnings [33] [100]. • Enforce users to complete some actions before allowing click through.
Hyperbolic discounting and updates (like sure things, waiting is difficult)	People, if given choice between two similar rewards, often give preference to sooner-smaller reward over later-larger reward.	• Provide information on the purpose of the patch. • Make the consequences/cost of neglecting the patch more salient. • Reduce the degree to which the non-instant reward is discounted. • Send reminders to update. • Introduce blocking off time for the patch.
Scarcity and access control management	The context of scarcity (shortage of time and money) introduces psychological burden and inhibits cognitive power (i.e., cognitive tunnelling).	• Use automation for access control management, wherever possible. • Make automatic expire after a certain time as default.
Congruence heuristic and risk assessment	People's tendency to over-rely on their initial belief and look only for confirmatory information while simultaneously ignoring alternative beliefs (i.e., ignore the beliefs that disapprove their initial belief)	• Make alternative beliefs (or security risks potentially unknown to them) salient.

Underestimating predictability and passwords	People are incredibly predictable in how they choose to comply with inconvenient norms. Further, they are prone to underestimating their predictability and similarity to others in their methods of compliance.	• Suggest randomly selected dictionary words as the base of the password, with special characters or number placement that defies expected patterns.
Hassle factors, status quo bias, and multi-factor authentication (MFA)	Even seemingly minor inconveniences or annoyances can act as *hassle factors* (i.e., anything that prevents from doing work efficiently and effectively). People exhibit preferences for the status quo or the current state of affairs.	• The recommended security features are pre-selected or given as the default option (to address status-quo bias); however, users with other preferences are allowed to opt-out (to address hassle factors).
Social proof and security measures	People who are unclear about what to do in a given scenario replicate the activities of others around them, even if there is no reason to believe they are doing the smart, or right thing.	• Without any *subjective framing*, simply present the specific number of co-workers who use the security features.

Interestingly, to complement both the MINDSPACE framework and the Nudge theory, the Behaviour Insights Team [41] developed the EAST framework. The four constituents or principles of this framework are **E**asy, **A**ttractive, **S**ocial, and **T**imely (EAST). The framework focuses on how the behavioural insights can be applied, for example, applying the nine influencers of the MINDSPACE or cyber nudges, Easy, Attractive, Social, and Timely. Some ways by which these four principles can be realised are mentioned in Table 7.

Table 7: Mechanisms to apply the EAST Framework

Constituent	Mechanisms to Apply
Easy	• Harness the power of defaults. • Reduce the "*hassle factor*" of taking up a service. • Simplify the messages.
Attractive	• Grab attention. • Highlight incentives (i.e., design rewards and sanctions for maximum effect).
Social	• Tap into the human instinct to align with others by showing them that most people perform the desired behaviour. • Use the power of the network. • Encourage people to make a commitment to others.
Timely	• Prompt people when they are likely to be most receptive. • Consider the immediate costs and benefits. • Help people plan their response to events. • Have as close to the behavioural choice as possible. • Reinforce regularly.

To sum up, different nudges can be designed and used to influence people to make correct security decisions or select the correct security options:

- *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, and*

- *implement the EAST (easy, attractive, social, and timely) framework to design and apply digital nudges.*

3.5.3 Cognitive and Cultural Biases

People possess many pre-existing biases, especially in the areas of cognition and culture. Due to the influence of these biases, their perceptions of risks are often distorted. For example, people may overestimate dread and unknown risks whereas underestimating the non-dreaded and known risks [33]. Ironically, these psychological biases are inescapable aspects of the human experience, shaped and impacted by past and present experiences. In cybersecurity, they influence people's security decision-making, strategies, and behaviour. Thus, it is necessary to understand these biases and consider appropriate steps to address the errors or skewness introduced in security decision-making processes by them. There are some studies that have exclusively explored such biases with the intent to identify them and determine in what ways they can impact cybersecurity decision-making and behaviour. Although there is no "*silver bullet*" to cope with and overcome all these biases, even simply being aware of them and acknowledging their effects on our decision-making is an important step towards their solution. Awareness of them could motivate some people to self-reflect and self-regulate their thinking, and practice security activities so as to gain more proficiency in how they process and do the activities. Moreover, it could also encourage the prevention of the aspects whenever possible, which can potentially cause or instigate or shape the biases. Last but not least, it will guide in applying suitable intrinsic/extrinsic motivations to address applicable biases, and apply recommended technological measures (e.g., message framing and usability in Table 6) that can minimise the impact of some biases [101].

One of the most comprehensive studies on cognitive and cultural biases for the *internalisation* of security policies is by Tsohou et al. [39]. It identified and analysed various biases that could potentially impact cybersecurity decision-making and behaviour. They identified and recommended to address namely the following cognitive biases: *affect heuristic, anchoring bias, confirmation bias, availability heuristic, optimism bias, loss aversion and hyperbolic time discounting*, and *risk perception and the psychometric paradigm*. Further, they mentioned addressing the cultural biases in the four cultural groups: *hierarchical, fatalists, individualists,* and *egalitarians,* depending on the cultural group being dealt with. As a result, they recommended considering these biases and their needful controls during the different phases of CSA programmes.

A report from ForcePoint [101] analysed six biases that can skew security decision-making and behaviour, which are: *aggregate bias, anchoring bias, availability bias, confirmation bias, the framing effect,* and *fundamental attribution error*.

Blau et al. [33] described various social psychological biases and factors that make people vulnerable to cyberattacks and also provided potential mitigations for them. Some psychological factors and biases raised by them are *affect heuristic, habituation, choice architecture, status quo bias and nudge users, loss aversion, hassle factor, availability heuristic, context of scarcity, congruence heuristic, command authority, salient cues, priming,* and *security by default.*

Bottomley et al. [36] asked to address cognitive biases such as *loss aversion, confirmation bias, hyperbolic discounting, affect heuristic, cognitive overloading,* and *bandwagon effect*, and to utilise psychological theories such as *social proof theory* and *intrinsic/ extrinsic motivation theory* in message framing.

To sum up, a consolidated list of cognitive, cultural, and other biases that can influence security decision-making and behaviour and need to be addressed, and some utilised for an effective CSA are presented in Table 8.

Table 8: List of cognitive and cultural biases as well as other factors that impact security decision making

Bias and Factor	Potential Mitigation
Affect Heuristic (*Decisions are heavily influenced by people's current emotions rather than concrete information; a tendency to underestimate or overestimate risks and costs associated with things based on whether an individual likes or dislikes the things, respectively.)*	• Concretise risk and make potential costs more salient by putting vivid information about specific threat consequences into browser warnings or search results. • Express risk in terms of relative frequency, which has a stronger impact on judgment than that expressed as a probability. • The assessments of costs and benefits of noncompliance and compliance are influenced by the images and feelings associated with them. o Avoid associating compliance (security or secure behaviour) with negative images and feelings. o Avoid associating noncompliance (unsecure behaviour) with positive images and feelings. • Refer to Table 6.
Aggregate bias (*A tendency to assume that trends observed in a group also apply to an individual.*)	• Use self-to-self, self-to-peer, and self-to-global comparisons to understand individual human behaviours and to provide personalised security solutions.
Anchoring effect *(A tendency to heavily rely on the initial piece of information given about a topic; once an anchor is set, an individual's subsequent arguments, estimates, values, and so on may differ from what s/he would have without the anchor.*)	• Use statistical analysis techniques to decrease the impact of overly weighted early judgments in favour of balancing the impact of new and critical information into the decision paradigm.
Authority bias *(A tendency to attribute greater accuracy to the opinion of an authority figure and be more influenced by that opinion.*)	• Refer to '*Messenger'* in the MINDSPACE framework (Table 5)—use trustworthy messenger with expertise in the security domain.
Availability heuristic (*A tendency to use information that comes to mind quickly and easily when making decisions about the future.*)	• Take the help of technology and data to understand the probabilities of various types of threats (e.g., warnings and notifications from security software, email system, and web browser). • Values the advice and recommendations of security experts and personnel.
Bandwagon effect *(A tendency to do something, regardless of their own beliefs, simply because other people are doing it.)*	• Utilise social proof theory (Refer to Table 2) —praise publicly the people performing well in security behaviour. • Refer to '*Norms'* of the MINDSPACE framework (Table 5)
Choice architecture *(Decision can be impacted by the ways choices are presented to them, for example, the number of choices, the manner in which attributes are described, and the presence of a default.)*	• An easy way could be to remove the choice altogether and automate the security activities [102], wherever possible. • Provide security choices that fail safely [103]. • Facilitate with clear and concise information on the benefits of each security choice so as to help in selecting the most relevant option.
Cognitive overloading *(A situation that can occur when too many stimuli demand attention at the same time.)*	• Focus on one task at a time and eliminate distractions. • Incorporate two-ways communication to be used for discussion with peers and instructors in order to clarify the confusion. • Refer to Table 2.
Correspondence bias or attribution effect *(A tendency to overattribute personality traits and under attribute the situation or context to explain behaviour.)*	• Get personal insight and practice empathy.

Confirmation bias (*A tendency to search for, interpret, favour, and recall information in a way that confirms or supports one's prior beliefs or values.)*	• Foster creative and flexible thinking, in particular, the ability and willingness to consider and approach issues from different perspectives. • Create an environment where teams can be comfortable with pushing each other's beliefs. • Use people and technology to facilitate mental exercises such as thinking backward, role-playing, devil's advocacy, and learning from surprising events. • Utilise the compromise effects (i.e., choose an intermediate option over the extremes). • Refer to Table 2.
Congruence heuristic *(A tendency to over rely on testing the initial hypothesis (the most congruent one) while neglecting to test alternative hypotheses.)*	• Use or build tools that prompt decision-makers to examine alternate evidence. Presumably, the decision-makers will be less inclined towards biased evidence if the alternative evidence is made more salient. • Refer to Table 6.
Context of scarcity *(A tendency to draw towards things that are perceived to be exclusive.)*	• Automate the processes by leveraging defaults. • Provide access to options that are required on regular basis.
Framing effect *(A tendency to decide on options based on whether they are presented with positive or negative connotations.)*	• Utilise loss aversion. • Refer to Table 2.
Hassle factor *(Irritating, frustrating, and distressing demands that stress people and may impact their decision.)*	• Refer to Table 6.
Habituation (*A non-reinforced response to a stimulus decreases after repeated or prolonged presentations of that stimulus.***)**	• Refer to Table 6.
Hyperbolic time discounting *(A tendency to choose a smaller-sooner aware over a large-later award.)* **Present bias** *(A tendency to let immediate costs outweigh far-off, long-term benefits.)*	• Organisations assess the long-term benefits of security and consider security as an investment and not a cost [104]. • Minimise the immediate costs of unsecure online actions and make the future benefits of security practices more vivid. For example, an individual who intended to illegally watch TV shows from an unsafe website is stopped and asked for confirmation and reconfirmation with suitable warning messages that inform of the harms. • Refer to Table 6.
Loss aversion *(A tendency to avoid losses over acquiring equivalent gains.)*	• Refer to Table 2.
Optimism bias *(An inclination to overestimate the likelihood of encountering positive events and to underestimate the likelihood of experiencing negative events in the future.)*	• Make the benefits of security and compliance with security policies more obvious and significant. • Routine assessment of the security risks can help to adjust optimism bias.
Priming *(A phenomenon whereby exposure to one stimulus influences a response to a subsequent stimulus, without conscious guidance or intention.)*	• Include mechanisms in the browser, email interface, and other security tools' interface that redirect users' attention to the '*right'* salient cues (this will potentially stop them from referring to wrong and irrelevant salient cues).

	• Refer to Table 5.
Status quo bias *(A tendency to prefer things to stay as they are or that the current status of affairs remains the same.)*	• Set the prescribed security options as the default ("Default" of the MINDSPACE framework.) • Reduce the number of security options available; when there are many options to pick from, status quo bias might become more pronounced. • Make the least secure options more effort taxing so that this can demotivate people from choosing them, for example, multi-factor authentication can be set as default whereas for single-factor authentication the individual has to perform some operations in the settings. • Utilise the loss aversion bias (by explaining the consequences of security actions and inactions) to motivate change.
Cultural biases *(Different groups of people, such as hierarchists, egalitarians, fatalists, and individualists can have varying interpretations of security threats and risks. People from a group may overestimate certain risks over others.)*	Cybersecurity strategies should be designed on the basis of different cultural biases. These biases can be addressed using different mechanisms, for example, • hierarchists believe in a well-defined hierarchy and role, so they can be influenced by security expert opinions, • individualists believe in the individual initiative so they trust less on security expert's opinion; however, they are self-regulated so can be influenced provided they get to calculate or observe the results by themselves, • egalitarians give high importance to the good of their group, so relating security to the benefits of the group can be effective for them, • fatalists are hard to motivate but by using rewards they can be motivated [105].

3.5.4 Incentive

Security behaviours can be enacted using a tough or a soft approach [43]. A tough approach utilises negative incentives like threats of punishments and sanctions whereas a soft approach uses positive incentives like persuasion, praise, rewards, enjoyment, and positive feedback. Although both approaches have been recommended for CSA purposes, a high preference is given to the soft approach in general [12]. Many other studies have suggested using sanctions and rewards as motivating factors to drive security behaviour change [6] [40] [41] [2]. Also, studies on behavioural theories like GDT [27] and TRA/TBP [29] have established a positive effect of the *perceived severity of sanctions* and *perceived cost of non-compliance* on cybersecurity behaviour, respectively. The use of rewards and punishments for motivating security behaviour change is mainly based on the *Incentive Theory* [106], according to which actions or behaviours are largely fuelled by the prospect of an external incentive. However, it is often argued that security actions and behaviours fuelled by *extrinsic incentives* (outside causes like rewards, threats of sanctions and punishments) may not be long-lasting or result in sustainable behavioural change [107]. Moreover, the chance of diminishing effect or regression in behaviour is high if the reward is stopped, decreased, or kept unchanged for some time. Therefore, some studies emphasised intrinsic incentives (inner satisfaction from interest, enjoyment, feedback, and praise) over extrinsic incentives for long-term behaviour change [43] [2] [108] [109].

A study conducted by Herath & Rao [108] to test the impact of incentives on security behaviour found that security behaviours are motivated by both intrinsic and extrinsic motivators. Among extrinsic incentives, the *certainty of punishment* was found to have a positive effect on security behaviour whereas the *severity of punishment* negatively affected security behaviour intentions. This study supported the role of punishments and sanctions in encouraging security behaviour, however, it also emphasised that their intensity should not be too harsh. Similarly, among intrinsic incentives, the pressure exerted by subjective norms and peer behaviours were found to be strong influencers of security behaviour change. Perceived effectiveness of actions was also found to play an important role in encouraging the adoption of security behaviour. The strong and positive influence of peer behaviour and pressure in enhancing cybersecurity behaviour has been supported by many other studies like Li et al. [109], Kirlappos et al. [43], and Modic & Anderson's [110]. This effect of peer pressure and behaviour could be due to people's desire to improve their "*self-image*" [104] and a sense of self-worth gained from comparing themselves to their peers [110].

However, the value of incentives can fluctuate over time and in different contexts [111], therefore it is important to understand the importance of incentives to the audience before employing them for motivation.

To sum up, incentives can play a role in motivating cybersecurity attitude and behaviour change, however,

- *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, and*
- *use extrinsic incentives when an urgent change is required.*

3.6 Usable Security

In simple terms, "*usable security*" refers to making the security products and processes usable for users. Since the CyberSec4Europe project has a deliverable report D3.5 [42] exclusively discussing the various aspects of the topic, this report does not want to delve into the topic. Here in this section, we have simply tried to establish the need for usable security as a motivating factor for security behaviour change.

It is not always that people are uninterested in changing security behaviour. Often impossible demands and awkward behaviours [112] imposed by security products and processes, or badly fitting security mechanisms (that put an additional burden by increasing friction between security and productivity) [43], inhibit them from doing so. This has also been shown in the study by Dykstra and Paul [113] and Kirlappos et al. [43], which found that fatigue, frustration, cognitive overload, and disruption caused due to cybersecurity operations are a few of the many factors that demotivate people from adopting cybersecurity behaviour or motivate them to embrace ad-hoc solutions. Thus, it is of utmost importance to minimise the impact of such demotivating factors through different means while designing security products, processes, and guidelines. Security professionals must consider the fact that "*security is rarely the primary concern of users*" [112] so security products, processes, and guidelines designed must not significantly hinder the primary task of the users.

Some studies with suggestions for improving the usability of CSA materials are, for example, Modic and Anderson [110] who suggested using non-technical language in security warnings; Bada et al. [6] who suggested making CSA contents interesting, current, easy to follow (so that even beginners are able to understand and practice), and directed to the audience; and Mayer et al. [56] who suggested using non-technical terms, positive phrasing, and relative frequencies whenever possible in password awareness-raising materials. Many usability suggestions for nudging purposes in CSA have been presented in Table 6. However, a more comprehensive list of factors that can be relevant for improving the usability of CSA contents and materials is included in Deliverable D3.19 [31]. Also, for more details on usable security and privacy methods, we recommend referring to CyberSec4Europe's deliverable report D3.5 [42].

To sum up, in order to facilitate and motivate security behaviour change, *make use of (or prefer to use) security products/processes/guidelines that were designed with usability in mind.*

3.7 Human Traits

Many studies have worked on establishing the correlation between cybersecurity behaviour intention with human traits.

Gratian et al. [114] used a survey to test the impact of human traits, namely, demographics (age, gender, role, academic major, national culture, and professional experience), personality traits (Big five personality traits), risk raking preferences (ethical, financial, health/safety, recreational, and social), and decision making styles (rational, avoidant, dependent, intuitive, spontaneous) on selected basic cybersecurity behaviour (device securement, password generation, proactive awareness, and software update). Their results revealed the gender to be significantly correlated to the other three behaviour intentions except for device securement. More specifically, females showed weaker behaviour intentions for them. Of course, other demographic traits are also found to be mildly correlated, for example, the age group of 18-25 and humanities majors showed a weaker correlation to security behaviour intentions. Among the personality traits, extraversion showed a significant correlation to device securement and conscientiousness to the remaining security behaviour intentions. Next, individuals willing to take health/safety risks are found to be poor in password generation and software updates, and in like manner those willing to take ethical risks are poor in proactive awareness. However, individuals willing to take financial risks are good at password generation. Finally, rational decision-making is positively correlated to device securement, proactive awareness, and software updating. And supporting avoidant decision making is positively correlated to password generation. However, spontaneous decision-making is negatively correlated to proactive awareness and software updates.

Kajzer et al. [40] used a survey to evaluate the effect of the five most popular message themes (*deterrence*—focuses on sanctions and punishments; *morality*—focuses on righteousness and societal norms; *regret*—focuses on negative consequences; *feedback*—focuses on providing information regarding behaviour, and *incentive*—focuses on rewards and personal gains) on individuals based on seven personality traits (the Big Five—extraversion, agreeableness, openness, conscientiousness, and neuroticism, Machiavellianism, and social desirability). In the evaluation, they choose age, gender, and security knowledge as control variables. Some significant associations found between message themes and personality traits are:

- *deterrence* — agreeableness (positive), neuroticism (positive), Machiavellianism (negative)
- *morality*—agreeableness (positive), social desirability (negative), Machiavellianism (negative)
- *regret*— agreeableness (positive), openness (negative), Machiavellianism (negative)
- *feedback*—openness (negative), extraversion (positive), agreeableness (positive), conscientiousness (positive), and neuroticism (positive)
- *incentive*— social desirability (positive), openness (negative)

McCormac et al. [115] used a survey to determine the effect of individual factors, namely demographics and personality traits (Big Five personality traits), on information security awareness. To measure the level of the participants' awareness, they used the Human Aspects of Information Security Questionnaire (HAIS-Q) [116], a well-validated questionnaire designed for the purpose. Their results showed that age (older people are more risk-averse in comparison to younger people), gender (females are more susceptible to phishing attacks than males), and agreeableness (positively related to the use of security software) to have a relation to information security awareness.

Finally, Moustafa et al. [100] identified different underlying personality, cognition, and behavioural traits in individuals that determine and differentiate their cybersecurity behaviours, namely, procrastination, impulsivity, future thinking, and risk-taking nature.

To sum up, CSAs need to consider human traits and *use relevant demographic information; personality, cognition, and behavioural traits; and decision-making styles to personalise CSA initiatives*.

4 Factors to Influence Security Attitude and Behaviour

Table 9 contains the consolidated results from the review of the papers. But upon further analysis of the results, the suggestions are found mainly targeting seven features, shown in Figure 3 and explained next.

Table 9: Consolidated list of factors and suggestions for influencing security attitude and behaviour change

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 exaggerate 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 descriptive format for the message presentation, except for the organisational awareness where 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 (courteousness in language), 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 part 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 are suitable for the content being communicated, the target audience group (the channels should best fit the content, and the audience should feel comfortable and preferable to use them) and have high information richness and 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 progress in multiple stages, and use persuasion techniques (logic, emotion, moral and ethics, well-beings, 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., uses media suitable for the learners, includes feedback interventions, provides autonomy in learning processes/flexible learning modes, is entertaining to learn, involves social interactions, provides role-specific and relevant examples, uses up-to-date content, uses short and comprehensible modules, and implements multi-delivery methods).
Persuasion Principle	• Provide plausible arguments on how the audience benefits by changing security attitudes or behaviour, use attention-grabbing message (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 response.
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 CSA initiatives.

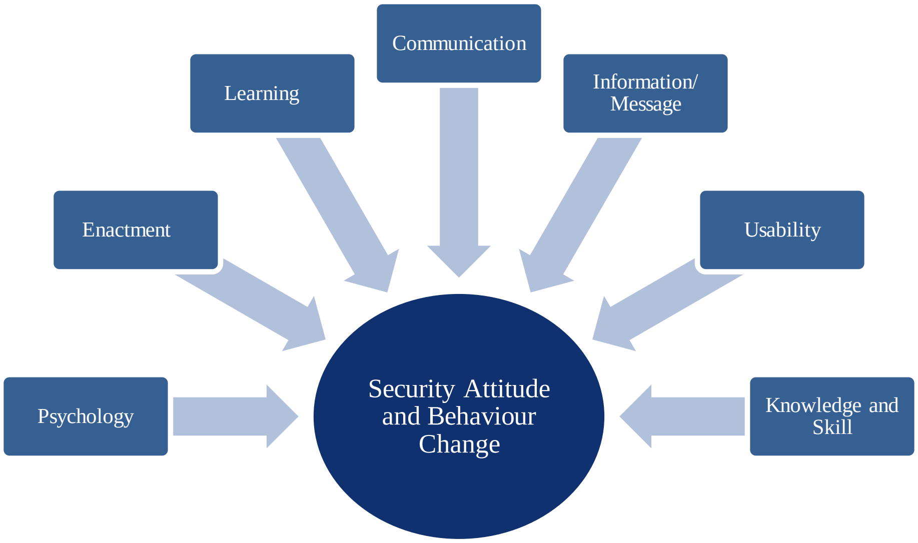

Figure 3: Features targeted by past studies to influence security attitude and behaviour

4.1 Psychology

- Factors that could need *addressing* to encourage attitude and behaviour change: affect heuristic, aggregate bias, anchoring effect, availability heuristic, cognitive overloading, correspondence bias or attribution effect, confirmation bias, congruence heuristic, hassle factor, habituation, hyperbolic time discounting or present bias, optimism bias, priming, cultural biases, and ego.
- Factors that could be *utilised* to encourage attitude and behaviour change: authority bias, bandwagon effect, choice architecture, the context of scarcity, framing effect, loss aversion, status quo bias, reciprocation, commitment and consistency, social proof, liking, authority, scarcity, and connecting the issue with a real-life problem.

4.2 Enactment

- A high value of these factors *encourages* attitude and behaviour change: perceived severity, perceived benefits of compliance, perceived severity of sanctions, perceived cost of non-compliance, subjective norms, extrinsic incentives valuable at the given time and context (rewards and sanctions), and intrinsic incentives valuable at the given time and context (praise, enjoyment, and positive feedback).
- A high value of these factors *discourages* attitude and behaviour change: response cost, and perceived cost of compliance.

4.3 Learning

- Factors that *encourage* attitude and behaviour change: content (community- centred learning content, tailored and personalised learning content); learning approach (group-oriented learning approach, experiential learning, stage-wise learning approach, instrumental learning, autonomy and ownership over learning, social learning and interaction, educate through entertainment); evaluation (communication-based evaluation, e.g., positive feedback, peer-based feedback).

4.4 Communication

- Factors that *encourage* attitude and behaviour change: credible communicator (trustworthy, expert, certified professional, authority), two-way communication, feedback and interaction, suitable communication channel (preferable and comfortable to the audience, non-technocratic, best fit the content to be communicated, and support information-rich media).

4.5 Information/ Message

- Factors that *encourage* attitude and behaviour change: relevant (what needs to be known), up to date, correct, unbiased, clear, concise, concrete, and complete information; polite presentation; salient presence; descriptive or prescriptive (for organisation) format; positively phrased and framed; realistic perspective, and compelling message with clear calls for doable actions.

4.6 Usability

- A high value of these factors *encourages* attitude and behaviour change: response efficacy, perceived usefulness, and perceived ease of use.
- Factors that *encourage* attitude and behaviour change: nudging (relevant warning messages-coping appraisal message, comping and threat appraisals combined message, graphical nudges, use of male anthropomorphic characters); security by default, a personification of characters (attackers and saviours), placement of information (important information at beginning and end), simple and understandable language, and personalised content and strategy.

4.7 Knowledge and Skill

- A high value of this factor *encourages* attitude and behaviour change: self-efficacy.
- Factors that *encourage* attitude and behaviour change: grouping of the audience (based on security beliefs, expertise level, and other relevant human traits, e.g., demographic information; personality, cognition, and behavioural traits; and decision-making styles).

5 Conclusions and Future Work

This report elicited and presented the list of factors that should be addressed and utilised depending on the need to influence cybersecurity attitude and behaviour change. The factors in Table 9 have been derived from multiple disciplines, namely,

- Behavioural theory,
- Framing theory,
- Communication theory,
- Pedagogical approach,
- Social psychology and behavioural economics (persuasion principle, cognitive and cultural biases, nudge theory, and incentive),
- Usable security, and
- Human traits

In addition to the list of factors, the report also includes potential mitigation measures through which those factors could be addressed or utilised in practice for CSA purposes. Although the list contains numerous factors that can influence security attitudes and behaviour, upon their further analysis, they are found to target seven features, namely

- psychology,
- enactment,

- learning,
- communication,
- information/ message,
- usability, and
- knowledge and skill.

The methodology used for this study is a non-systematic literature review, mainly for its flexibility to allow exploration of multiple disciplines and sectors.

The outcomes of this report can be of value to CSA professionals and organisations who intend to design, develop, and implement CSA programmes. Furthermore, the knowledge could be useful also for those who generate requests for awareness designers as well as for any subject who wishes to evaluate the effectiveness of the adopted security measures.

There are some limitations to the usefulness of the resulting list. Firstly, it may not be practically feasible to consider such a larger number of factors in designing CSA initiatives. Secondly, all the factors cannot be of the same relevance; some factors could be more relevant and effective in comparison to others. Finally, the list may have overlooked some important factors and included factors that may no longer be relevant. Therefore, to elicit the most important factors and also validate them for relevancy and applicability, we plan to use the Delphi method using an expert panel. The final list of factors and other findings from the Delphi method will be presented in D9.26, the third and final report for the "*Awareness effectiveness study*".

6 References

[1] S. Chaudhary, V. Gkioulos und D. Goodman, "D9.11 SME Cybersecurity awareness programme 2," CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2021/05/D9.11-SME-cybersecurity-awareness-programme-2-FINAL-submitted-1.pdf (11 November 2021, last accessed).

[2] M. T. Siponen und J. Kajava, "Ontology of Organisational IT Security Awareness- From Theoretical Foundations to Practical Framework," in *Seventh IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises*, Stanford, CA, USA, 17-19 June 1998.

[3] S. Furnell und I. Vasileiou, "Security education and awareness: Just let them burn?," *Network Security*, Bd. 2017, Nr. 12, pp. 5-9, December 2017.

[4] H.A.Kruger und W.D.Kearney, "A prototype for assessing information security awareness," *Computers & Security*, Bd. 25, Nr. 4, pp. 289-296, June 2006.

[5] S. Chaudhary, "D9.13 Awareness effectiveness study 1," CyberSec4Europe, https://cybersec4europe.eu/wp-content/uploads/2021/02/D9.13-Awareness-effectiveness-study-v1.0-submitted.pdf (21 November 2021, last accessed).

[6] M. Bada, A. M. Sasse und 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, 26 February 2015.

[7] G. Stewart und D. Lacey, "Death by a thousand facts: Criticising the technocratic approach to information security awareness," *Information Management & Computer Security,* Bd. 20, Nr. 1, pp. 29-38, 2012.

[8] ENISA, "Information security awareness initiatives: Current practice and the measurement of success," European Network and Information Security Agency, Athens, Greece, July 2007.

[9] EPIGNOSIS, "Cybersecurity training may be broken, new survey reveals: 61% of employees who have received training failed a basic test," Available online, https://www.epignosishq.com/cybersecurity_training_survey/ (22 November 2021, last accessed).

[10] I. Winkler und S. Manke, "7 reasons for security awareness failure," Available online: https://www.csoonline.com/article/2133697/7-reasons-for-security-awareness-failure.html (22 November 2021, last accessed).

[11] L. Spitzner, "Top 3 Reasons Security Awareness Training Fails," Available online: https://www.sans.org/blog/top-3-reasons-security-awareness-training-fails/ (5 August 2021, last accessed).

[12] Hoxhunt, "How to create behaviour change with security awareness training? A practical guide," Available online: https://pages.hoxhunt.com/hubfs/eBooks/How%20to%20create%20behaviour%20change%20with%20security%20awareness%20training_.pdf (20 August 2021, last accessed).

[13] ENISA, "The new users' guide: How to raise information security awareness," ENISA, Athens, Greece, November 2010.

[14] A. Christiano und A. Neimand, "Stop Raising Awareness Already," *Stanford Social Innovation Review,* pp. 34-41, Spring 2017.

[15] A. Whitten und J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *8th USENIX Security Symposium*, Washington, D.C., USA, August 1999.

[16] K.-P. Yee, "Aligning Security and Usability," *IEEE Security & Privacy*, Bd. 2, Nr. 5, pp. 48-55, Sept-Oct 2004.

[17] M. E. Kabay, "Using Social Psychology to Implement Security Policies," in *Computer Security Handbook*, John Wiley & Sons, 2002, pp. 35.1-35.22.

[18] J. Barker, "The Human Nature of Cybersecurity," *Educause Review,* pp. 11-17, 20 May 2019.

[19] ENISA, "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," ENISA, Athens, Greece, December 2018.

[20] A. Booth, A. Sutton und D. Papaioannou, Systematic Approaches to a Successful Literature Review, SAGE Publications, 2012.

[21] CyberSec4Europe, "Deliverables," Available online: https://cybersec4europe.eu/our-results/deliverables/ (19 January 2022).

[22] A. Paez, "Gray literature: An important resource in systematic reviews," *Journal of Evidence-Based Medicine*, Bd. 10, Nr. 3, pp. 233-240, August 2017.

[23] H. R. Kwon und E. A. Silva, "Mapping the Landscape of Behavioural Theories: Systematic Literature Review," *Journal of Planning Literature*, Bd. 35, Nr. 2, 2020.

[24] B. Lebek, J. Uffen, M. Neumann, B. Hohler und M. H. Breitner, "Information security awareness and behaviour: a theory-based literature review," *Management Research Review*, Bd. 37, Nr. 12, November 2014.

[25] S. F. Austin und M. D. Faries, "Why We Don’t “Just Do It”: Understanding the Intention-Behaviour Gap in Lifestyle Medicine," *American Journal of Lifestyle Medicine*, Bd. 10, Nr. 5, pp. 322-329, September 2016.

[26] I. Woon, G.-W. Tan und R. Low, "A Protection Motivation Theory Approach to Home Wireless Security," in *International Conference on Information Systems*, Las vegas, NV, USA, 11-14 December 2005.

[27] J. D'Arcy, A. Hovav und D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research*, Bd. 20, Nr. 1, pp. 79-98, March 2009.

[28] C. M. Jones, R. V. McCarthy und B. Muujtaba, "Utilizing the technology acceptance model to assess employee adoption of information systems security measures," *Issues in Information*, Bd. 11, Nr. 1, pp. 9-16, 2010.

[29] B. Bulgurcu, H. Cavusoglu und I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly*, Bd. 34, Nr. 3, pp. 523-548, September 2010.

[30] P. Mayer, A. Kunz und M. Volkamer, "Reliable Behavioural Factors in the Information Security Context," in *ARES*, Reggio Calabria, Italy, 29 September-1 October 2017.

[31] S. Chaudhary, S. Pape, M. Kompara, G. Kavallieratos und V. Gkioulos, "D3.19 Guidelines for Enhancement of Societal Security Awareness," CyberSec4Europe, Brussel, Belgium, February 2022.

[32] M. A. Arain, R. Tarraf und A. Ahmad, "Assessing staff awareness and effectiveness of educational training on iT security and privacy in a large healthcare organisation," *Journal of Multidisciplinary Healthcare*, Bd. 2019, Nr. 12, pp. 73-81, 2019.

[33] A. Blau, A. Alhadeff, M. Stern, S. Stinson und J. Wright, Deep Thought: A Cybersecurity Story, New York, NY, USA: Ideas42, 2017.

[34] H. Bruijn und M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Government Information Quarterly,* Bd. 34, Nr. 1, pp. 1-7, January 2017.

[35] K. S. Bordens und I. A. Horowitz, "Persuasion and Attitude Change," in *Social Psychology*, New York, NY, USA, Taylor & Francis Group, 2002, pp. 191-234.

[36] E. Bottomley, C. Munnelly, L. Tryl und S. Wride, "What makes a successful campaign?," *Available online: https://cms.wellcome.org/sites/default/files/public-first-literature-review.pdf (19 August 2021, last accessed).*

[37] C. Chipperfield und S. Furnell, "From security policy to practice: Sending the right messages," *Computer Fraud & Security,* pp. 13-19, March 2010.

[38] C. W. Yoo, G. L. Sanders und R. P. Cerveny, "Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance," *Decision Support Systems,* Bd. 108, p. 107–118, 2018.

[39] A. Tsohou, M. Karyda und S. Kokolakis, "Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programmes," *Computers & Security,* Bd. 52, pp. 128-141, 2015.

[40] M. Kajzer, J. D'Arcy, C. R. Crowell, A. Striegel und D. V. Bruggen, "An exploratory investigation of message person congruence in information security person congruence in information security awareness campaigns," *Computers & Security,* Bd. 43, pp. 64-76, 2014.

[41] The Behavioural Insights Team, "EAST: Four Simple Ways to Apply Behavioural Insights," Available online: https://www.bi.team/wp-content/uploads/2015/07/BIT-Publication-EAST_FA_WEB.pdf (12 November 2021, last accessed).

[42] K. Halunen et al., "D3.5 Usable security & privacy methods and recommendations," CyberSec4Europe, Brussel, Belgium, 31 January 2020.

[43] I. Kirlappos, S. Parkin und M. A. Sasse, ""Shadow security" as a tool for the learning organisation," *ACM SIGCAS Computers and Society,* Bd. 45, Nr. 1, p. 29–37, February 2015.

[44] P. Dolan, M. Hallsworth, D. Halpern, D. King und I. Vlaev, "Influencing behaviour: The MINDSPACE way," *Journal of Economic Psychology,* Bd. 33, pp. 264-277, 2012.

[45] Relevance, "Message Framing: The Art of Persuasion," Available online: https://www.relevance.com/message-framing-the-art-of-persuasion/ (4 April 2022, last accessed).

[46] S. M. Smith und R. E. Petty, "Message Framing and Persuasion: A Message Processing Analysis," *Personality and Social Psychology Bulletin,* Bd. 22, Nr. 3, pp. 257-268, March 1996.

[47] D. D. Rucker, R. E. Petty und P. Briñol, "What's in a frame anyway? A meta-cognitive analysis of the impact of one versus two-sided message framing on attitude certainty," *Journal of Consumer Psychology,* Bd. 18, Nr. 2, pp. 137-149, April 2008.

[48] R. M. Entman, "Framing: Towards clarification of a fractured paradigm," *Journal of Communication,* Bd. 43, Nr. 4, pp. 51-58, 1993.

[49] D. Kahneman und A. Tversky, "Choices, Values, and Frames," *American Psychologist,* Bd. 39, Nr. 4, pp. 341-450, April 1984.

[50] M. Edelman, "Contestable categories and public opinion," *Political Communication,* Bd. 10, Nr. 3, pp. 231-242, 1993.

[51] S. A. Fisher und D. R. Mandel, "Risky-choice framing and rational decision-making," *Philosophy Compass*, Bd. 16, Nr. 8, August 2021.

[52] M. Siponen, "Five dimensions of information security awareness," *Computer and Society,* Bd. 31, Nr. 2, pp. 24-29, 2001.

[53] J. Baird und J. Stull, The Seven C's of Communication., Englewood Cliffs, NJ: Prentice Hall, 1992.

[54] KnowBe4, "Developing a Cybersecurity Culture," Available online: https://www.securityadvisor.io/developing-a-cybersecurity-culture/#:~:text=According%20to%20Stanford%20University%20Behaviour,actions%20set%20the%20ground%20rules. (1 April 2022, last accessed).

[55] D. Maheswaran und J. Meyers-Levy, "The influence of message framing and issue involvement," *Journal of Marketing Research*, Bd. 27, Nr. 3, pp. 361-367, August 1990.

[56] P. Mayer, C. Schwartz und M. Volkamer, "On the Systematic Development and Evaluation Of Password Security Awareness-Raising Materials," in *34th Annual Computer Security Applications Conference*, San Juan, PR, USA, 3-7 December, A 2018.

[57] S. K. Katsikas, "Health care management and information system security: Awareness, training or education?", *International Journal of Medical Informatics*, Bd. 60, pp. 129-135, 2000.

[58] B. B. Murdock, "The serial position effect of free recall," *Journal of Experimental Psychology*, Bd. 64, Nr. 5, p. 482–488, 1962.

[59] S. M. Glynn, "Cognitive Processes Involved in Text Learning," in *Annual Meeting of the American Educational Research Association,* Montreal, Canada, 1983.

[60] H. D. Lasswell, "The structure and function of communication in society," in *Bryson, L. (ed.) The Communication of Ideas*, New York, USA, Harper and Brothers, 1948, pp. 37-51.

[61] A. Monroe, Monroe's Principles of Speech, Scott Foresman, 1951.

[62] L. Spitzner, D. deBeaubien und A. Ideboen, "The rising era of awareness training," SANS Security Awareness Report, Bethesda, MD, USA, 2019.

[63] J. M. Haney und W. G. Lutters, "Skills and characteristics of successful cybersecurity advocates," in *Workshop on Security Information Workers, Symposium on Usable*, Santa Clara, CA, USA, 12-14 July, 2017.

[64] D. House und G. Giordano, "Politeness in security directives: Insights in browser compliance for the human element," *Computers & Security,* Bd. 99, 2020.

[65] R. Shaw, C. C. Chen, A. L. Harris und H.-J. Huang, "The impact of information richness on information securit awareness training effectiveness," *Computers & Education,* Bd. 52, Nr. 1, pp. 92-100, 2009.

[66] R. Daft und R. Lengel, "Information richness: A new approach to managerial behaviour and organisational design," *Research in Organisational Behaviour,* Bd. 6, pp. 191-233, 1984..

[67] AlbertCaballero, "Security Education, Training, and Awareness," in *Computer and Information Security Handbook,* Burlington, Massachusetts, USA, Morgan Kaufmann, 2017, pp. 497-505.

[68] C. M. B. Turner und C. F. Turner, "Analyzing the impact of experiential pedagogy in teaching socio-cybersecurity: cybersecurity across the curriculum," *Journal of Computing Sciences in Colleges,* Bd. 34, Nr. 5, p. 12–22, April 2019.

[69] M. Karjalainen, T. Kokkonen und S. Puuska, "Pedagogical Aspects of Cyber Security Exercises," in *IEEE European Symposium on Security and Privacy Workshops*, Stockholm, Sweden, 17-19 June 2019.

[70] S. Hart, A. Margheri, F. Paci und V. Sassone, "Riskio: A Serious Game for Cyber Security Awareness and Education," *Computers & Security*, Bd. 95, August 2020.

[71] M. Karjalainen und M. Siponen, "Toward a New Meta-Theory for Designing Information Systems (IS) Security Training Approaches," *Journal of the Association for Information Systems,* Bd. 12, Nr. 8, pp. 518-555, August 2011.

[72] M. E. Thomson und R. v. Solms, "Information security awareness: educating your users effectively," *Information Management & Computer Security,* Bd. 6, Nr. 4, p. 167–173, 1998.

[73] I. Vasileiou und S. Furnell, "Personalising Security Education: Factors Influencing Individual Awareness and Compliance," in *International Conference on Information Systems Security and Privacy,* Funchal, Madeira, Portugal, 22-24 January 2018.

[74] C. L. Stevenson, Ethics and Language, New Haven, USA: Yale University Press, 1944.

[75] P. Story, D. Smullen, Y. Yao, A. Acquisti, L. F. Cranor, N. Sadeh und F. Schaub, "Awareness, Adoption, and Misconceptions of Web Privacy Tools," *Proceedings on Privacy Enhancing Technologies,* Bd. 3, pp. 308-333, July 2021.

[76] S. Chaudhary, Y. Zhao, S. Mystakidis, E. Berki, J. Valtanen, L. Li und M. Helenius, "A Cross-cultural and Gender-based Perspective for Online Security: Exploring Knowledge, Skills and Attitudes of Higher Edcuation Students," *IADIS International Journal on WWW/Internet,* Bd. 13, Nr. 1, 2015.

[77] Y.-Y. Chan und V. K. Wei, "Teaching for Conceptual Change in Security Awareness," *IEEE Privacy & Security,* Bd. 6, pp. 67-69, November/December 2008.

[78] E. E. Ekon und N. B. Edem, "Conceptual Change Pedagogy and Its Effects On Students' Cognitive Achievement and Interest in Biology," *International Journal for Cross-Disciplinary Subjects in Education,* Bd. 9, Nr. 2, pp. 3407-3413, June 2018.

[79] Y.-. Chan und V. K. Wei, "Teaching for Conceptual Change in Security Awareness: A Case Study in Higher Education," *IEEE Security & Privacy,* Bd. 7, Nr. 1, pp. 68 - 71, 2009.

[80] S. N. Baviskar, R. T. Hartle und T. Whitney, "Essential Criteria to Characterize Constructivist Teaching: Derived from a review of the literature and applied to five constructivist-teaching method articles," *International Journal of Science Education,* Bd. 31, Nr. 4, pp. 541-550, 2009.

[81] B. Gardner und V. Thomas, "Why Current Programmes Don't Work," in *Building an Information Security Awareness Programme: Defending Against Social Engineering and Technical Threats,* Waltham, MA, USA, Syngress, 2014, pp. 39-44.

[82] D. Kahneman, Thnking Fast and Slow, New York, USA: Farrar, Straus and Giroux, 2013.

[83] S. Chan, K. Duckworth und S. Chaiken, "Motivated Heuristic and Systematic Processing," *Psychological Inquiry,* Bd. 10, Nr. 1, pp. 44-49, 1999.

[84] E. T. Higgins, "Knowledge activation: Accessibility, applicability, and salience," in *E. T. Higgins & A. W. Kruglanski (Eds.), Social psychology: Handbook of basic principles*, New York, NY, USA, The Guilford Press, January 1996, p. 133–168.

[85] J.-W. H. Bullee, ·. Montoya, W. Pieters, M. Junger und P. H. Hartel, "The persuasion and security awareness experiment: reducing the success of social engineering attacks," *Journal of Experimental Criminology*, Bd. 11, p. 97–115, 2015.

[86] H. A. Simon, "Theories of Bounded Rationality," in *C.B. McGuire and Roy Radner (eds.) Decision and Organisation*, Amsterdam, The Netherlands, North Holland Publishing Company, 1972, pp. 160-176.

[87] A. Luttrell, P. Brinol und R. E. Petty, "Mindful Versus Mindless Thinking and Persuasion," in *The Wiley Blackwell Handbook of Mindfulness*, Hoboken, NJ, USA, John Wiley & Sons, Ltd., 2014, pp. 258-278.

[88] R. B. Cialdini, Influence: The Psychology of Persuasion, Harper Collins, 2006.

[89] L. Coventry, P. Bridge, J. Blythe und M. Tran, "Using behavioural insights to improve the public's use of cyber security best practices," Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/309652/14-835-cyber-security-behavioural-insights.pdf (17 August 2021, last accessed).

[90] H. Mills, Artful Persuasion: How to Command Attention, Change Minds, and Influence People, New York, NY, USA: AMA Publications, 2000.

[91] E. Langer, A. Blank und B. Chanowitz, "The Mindlessness of Ostensibly Thoughtful Action: The Role of "Placebic" Information in Interpersonal Interaction," *Journal of Personality and Social Psychology,* Bd. 36, Nr. 6, pp. 635-642, 1978.

[92] C. Carpenter, F. J. Boster und K. R. Andrews, "Functional Attitude Theory," in *The SAGE handbook of persuasion: Developments in theory and practice*, Sage Publications, 2013, pp. 104-119.

[93] H. J.Wall, C. C. Campbell, L. K. Kaye, A. Levy und N. Bhullar, "Personality profiles and persuasion: An exploratory study investigating the role of the Big-5, Type D personality and the Dark Triad on susceptibility to persuasion," *Personality and Individual Differences*, Bd. 139, pp. 69-76, March 2019.

[94] R. E. Petty, John T. Cacioppo und R. Goldman, "Personal involvement as a determinant of argument-based persuasion," *Journal of Personality and Social Psychology,* Bd. 41, Nr. 5, p. 847–855, 1981.

[95] L. R. Fabrigar, J. R. Priester, R. E. Petty und D. T. Wegener, "The Impact of Attitude Accessibility on Elaboration of Persuasive Messages," *Personality and Social Psychology Bulletin,* Bd. 24, Nr. 4, pp. 339-352, April 1998.

[96] R. v. Bavel und N. Rodríguez-Priego, "Nudging Online Security Behaviour with Warning Messages: Results from an Online Experiment," Available online: https://publications.jrc.ec.europa.eu/repository/handle/JRC103223 (12 November 2021, last accessed).

[97] R. v. Bavel, N. Rodríguez-Priego, J. Vila und P. Briggs, "Using protection motivation theory in the design of nudges to improve online security behaviour," *International Journal of Human-Computer Studies,* Bd. 123, pp. 29-39, 2019.

[98] K. Sharma, X. Zhan, F. F.-H. Nah, K. Siau und M. X. Cheng, "Impact of digital nudging on information security behaviour: an experimental study on framing and priming in cybersecurity," *Organisational Cybersecurity Journal: Practice, Process and People*, Bd. 1, Nr. 1, pp. 69-91, 2021.

[99] C. Suter, J. Armijo, J. Whitaker und M. Morgenstern, "Nudging for Cybersecurity," Available online: https://www.dayblink.com/wp-content/uploads/2019/08/Nudging-for-Cybersecurity-Final.pdf (12 November 2021, last accessed).

[100] A. A. Moustafa, A. Bello und A. Maurushat, "The Role of User Behaviour in Improving Cyber Security Management," *Frontiers in Psychology,* Bd. 12, June 2021.

[101] M. Cunningham, "Thinking About Thinking: Exploring Bias in Cybersecurity with Insight from Cognitve Science," Forcepoint, Herndon, Virginia, USA, 2020.

[102] R. Montesino und S. Fenz, "Information Security Automation: How Far Can We Go?," in *Sixth International Conference on Availability, Reliability and Security*, Vienna, Austria, 22-26 Aug. 2011.

[103] M. Gegick und S. Barnum, "Failing Securely," Cybersecurity & Infrastructure Security Agency, Rosslyn, Arlington, Virginia, USA, 05 December 2005.

[104] P. R. Trim und Y.-I. Lee, "The role of B2B marketers in increasing cyber security awareness and influencing behavioural change," *Industrial Marketing Management,* Bd. 83, p. 224–238, 2019.

[105] R. P. Nielsen, "Communicating with and Motivating High Fatalists," *The American Journal of Economics and Sociology,* Bd. 32, Nr. 4, pp. 337-350, October 1973.

[106] The Psychology Notes HQ, "The Incentive Theory of Motivation," Available online: https://www.psychologynoteshq.com/incentive-theory-of-motivation/ (07 May 2022, last accessed).

[107] U. Gneezy, S. Meier und P. Rey-Biel, "When and Why Incentives (Don't) Work to Modify Behaviour," *Journal of Economic Perspectives,* Bd. 25, Nr. 4, p. 191–210, Fall 2011.

[108] T. Herath und H.R.Rao, "Encouraging information security behaviours in organisations: Role of penalties, pressures and perceived effectiveness," *Decision Support Systems,* Bd. 47, Nr. 2, pp. 154-165, May 2009.

[109] L. Li, L. Xu, W. He, Y. Chen und H. Chen, "Cyber Security Awareness and Its Impact on Employee's Behaviour," in *International Conference on Research and Practical Issues of Enterprise Information Systems*, Vienna, Austria, 13-14 December 2016.

[110] D. Modic und R. Anderson, "Reading this may harm your computer: The psychology of malware warnings," *Computers in Human Behaviour,* Bd. 41, pp. 71-79, December 2014.

[111] S. L. Franzoi, Psychology: A Discovery Experience, Boston, MI, USA: Cengage Learning, 2014.

[112] M. A. Sasse und I. Flechais, "Usable Security: Why Do We Need It? How Do We Get It?," in *L.F. Cranor and S. Garfinkel (eds.) Security and Usability: Designing secure systems that people can use.*, Sebastopol, US, O'Reilly, 2005, pp. 13 - 30.

[113] J. Dykstra und C. L. Paul, "Cyber Operations Stress Survey (COSS): Studying fatigue, frustration, and cognitive workload in cybersecurity operations," in *11th USENIX Conference on Cyber Security Experimentation and Test*, Baltimore MD USA, 13 August 2018.

[114] M. Gratian, S. Bandi, M. Cukier, J. Dykstra und A. Ginther, "Correlating human traits and cyber security behaviour relations," *Computer & Security*, Bd. 73, pp. 345-358, 2018.

[115] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius und M. Pattinson, "Individual Differences and Information Security Awareness," *Computer in Human Behaviour*, Bd. 69, pp. 151-156, April 2017.

[116] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac und T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies," *Computers & Security*, Bd. 66, pp. 40-51, May 2017.