

Applying Behaviour Change Knowledge to Foster Secure Employee Behaviour: An Exploratory Study with Security and Security Awareness Practitioners

1st Rebecca Panskus
Ruhr University Bochum
Bochum, Germany
rebecca.panskus@rub.de

2nd M. Angela Sasse
Ruhr University Bochum
Bochum, Germany
martina.sasse@rub.de

3rd Karola Marky
Ruhr University Bochum
Bochum, Germany
karola.marky@rub.de

Abstract—Most organisations provide security awareness and training for their employees, through face-to-face sessions or online modules that explain risks and secure behaviours to mitigate them. In 2016, Beyer et al. [1] pointed out that the transmission of knowledge about risks and behaviours is not enough to establish secure behaviour. They proposed an *awareness maturity curve* as a theoretical framework consisting of seven stages of behaviour change to establish secure behaviour, and measures that organisations need to deploy in order to support their employees in the transition. In 2022, Sasse et al. proposed a revised version, the *security behaviour change curve* (SBCC) with 9 stages [2]. We briefly introduce the SBCC and explain the psychological and behavioural science concepts from which it is derived. We then describe an exploratory study with 25 experienced security and security awareness practitioners who we asked to apply the SBCC in order to design interventions in nine ideation workshops. Guided by a set of questions, they were asked to propose interventions for each stage for four hypothetical scenarios based on documented security behaviour issues. We found that practitioners overwhelmingly propose interventions they currently use – even if they have been shown to be ineffective – and try to fit them in the stages; creating suitable interventions on the stages of the SBCC guided by the concepts was a challenge. We provide a dataset of expert-ideated interventions for the four real-world security-critical behaviours, and supplementary guidelines for practitioners.

Index Terms—security behaviour change curve, security and security awareness practitioners, employee security

I. INTRODUCTION

In the digital age, information security is essential to organisations. Many attacks target employees to gain access to corporate systems [3], [4]. Organisations provide security awareness training (SAT) to raise awareness of risks, and teach their employees secure behaviours to manage these [4]. The overwhelming amount of training is delivered via web-based training packages; today, often in combination with simulated phishing campaigns. Over the past decade, research studies have raised doubt about whether this approach is effective in establishing secure behaviour among employees, e.g. [5], [6] and pointed out the hidden cost of deploying this training goes way beyond the training package itself [7].

The key problem is that providing employees with security knowledge through training packages once a year is

not enough to foster secure behaviour in the everyday work environment. Secure behaviour needs to become a habit – automatic behaviour triggered by a stimulus, rather than the outcome of a conscious thought process [8]. Habits require little cognitive effort [9] and are only slightly affected by stress, which leads to consistent reactions even under changing conditions [10]. Many employees bring their habits – secure or insecure – from their private lives to work [11]. Transforming insecure habits into secure ones can be a lengthy process, as updating habits requires repetition [12], [13]. To guide this process of fostering secure employee habits by behavioural change, Beyer et al. [1] developed the *awareness maturity curve* in 2016.

In follow-up work, the original curve was iteratively refined [14], and extended into the *security behaviour change curve* (SBCC) by Sasse et al. [2]. The SBCC is based on established psychological concepts including compliance budgets (see *Sect. II-C1a*), self-efficacy (see *Sect. II-C1b*), or intentional forgetting (see *Sect. II-C1c*). But the SBCC has not been evaluated with the key practitioners that would have to apply it: security and security awareness practitioners. In this paper, we first contextualize the extended SBCC to habit formation [8] and rewards for reinforcing habit formation [15], [16]. Second, we address the gap on missing evaluation by conducting an analysis of the SBCC with practitioners from the field of security and security awareness. We specifically investigated whether practitioners (a) can use the theoretical SBCC framework and (b) can use it to ideate behaviour change interventions for real-world security problems, considering the following core research question:

RQ: *How can the theoretical framework of the security behaviour change curve be applied by practitioners to security-critical behaviours?*

For this, we conducted nine workshops with a total of N=25 practitioners. During these workshops, our participants examined security-critical behaviours that they had recently observed in their organisations, and then followed the nine SBCC stages to ideate interventions for employees to adopt secure behaviour.

Our results show that our security and security awareness practitioners can use the SBCC to plan interventions. However, our results also show that their own established working habits lead them to propose mostly established interventions – such as phishing interventions, which have been shown to be ineffective (cf. *Sect. II-A*). And despite claiming to take an employee-centred approach, they use security jargon language that is not understood by laypeople [17]–[19].

This paper makes the following key contributions:

a) Breakdown of the Psychological Context: We broke down the psychological background of each SBCC stage to illustrate why each stage is important and how practitioners can apply them correctly when planning behaviour change interventions (see *Sect. II-C*).

b) Applicability of the SBCC & Interventions for Behaviour Change: Through nine workshop sessions with 25 practitioners from the field of security and security awareness, we present the first expert ideation of the SBCC. Our results show that our participants were able to ideate some new interventions for the different stages of the SBCC, and adapt some existing interventions, to support the formation of secure habits. Further, the workshops resulted in a collection of hypothetical plans for adopting four secure behaviours in organisations with real-world importance identified by our participants using the SBCC (see *Sect. IV & Tab. II*). These interventions can serve as guidance for other practitioners in their organisational context or motivate novel dedicated interventions.

c) Guidelines for Practitioners on Applying the SBCC: Based on the workshops’ results and the practitioners’ interaction with the SBCC, we derive essential guidance to support practitioners to use the SBCC in their organisations (see *Sect. V-A*).

II. BACKGROUND & RELATED WORK

This section first summarises related work on compliance, SAT and behaviour change in organisations. Next, we provide a detailed overview of the SBCC and its psychological basis.

A. Compliance, SAT and Behaviour Change in Organisations

Organisations currently purchase SAT, “[...] *any intervention, online or in-person, to increase employees’ security knowledge and/or to change their behaviour [...]*”, to guide their employees towards secure behaviour ([20], p.2667). In the U.S. between 2023 and 2025 at least 78.3% of companies implemented SAT [4].

One common SAT are simulated phishing campaigns (SPC). These SPCs aim to achieve a learning effect through teachable moments [21]. While management sees advantages in such campaigns, such as the quantifiability of clicks [22], the effectiveness of such training is a subject of controversy. SPCs can increase stress for individuals who click on simulated phishing emails [23]. However, participants who successfully reported the simulated phishing emails wished that SPC emails were sent more often, revealing a positive attitude towards

SPCs [23]. Similarly, Schiller et al. [24] found that employees had positive attitudes towards SPCs, but no concrete changes in employee behaviour were observed, which means that the actual SPC goal is not achieved. Volkamer et al. [25] revealed further problems with SPCs, as they can lead to distrust between employees and IT management. However, this has not been confirmed by more recent work [24]. Furthermore, on the downside, employees can develop a false sense of security, as they feel protected by the company due to training [5], [24], [26] or develop overconfidence both in their abilities and in the fact that mistakes in SPCs are without repercussions [27], having a countervailing effect on employees awareness.

Overall, research has shown that SATs have very limited effectiveness and a limited impact on employee awareness and behaviour [24], regardless of whether they are annual SATs or embedded SPCs [6]. From an economic perspective, SATs can also have hidden costs. Multiple costs that are not taken into account initially, can occur during the evaluation and procurement phase of an SPC [7]. These include high costs in person hour due to additional work and time required for management, resulting in increasing stress in the working environment and emotional strain [7]. Another factor leading to quality deterioration of relationship between employees and security departments is security friction [28], meaning that security tasks interfere with employees main tasks. Further consequences of SATs can include reduced self-efficacy among employees and lower trust in the organisation [25].

However, organisations consider SAT and simulated phishing necessary for compliance reasons, and CISOs and security awareness practitioners are expected to deliver it [22]. There is no doubt that most employees do not know about all risks and secure behaviours. But while “ticking the box” is often the most important priority for management [7], mandating that employees work through standard SATs does not lead to secure behaviour – actual compliance in the everyday working environment. This is largely because the secure behaviour causes friction with job routines [29] – many practitioners are aware of this, but claim to lack resources and backing from management, which is focused on compliance [28]. Unable to address security friction, practitioners tend to see it as an unavoidable cost of security and SAT as a means to persuade employees to accept it [22], [28]. The SBCC addresses the issues of traditional SATs, providing a foundation for the future development and implementation of effective SATs aimed at fostering secure behaviour among employees.

B. Behaviour Change Models

Over the past two decades, many different behaviour change models based on academic research have been developed. Concrete examples of models based on empirical research are the *Fogg Behaviour Model* (FBM) [30], the COM-B system by Michie et al. [31], and the choice architecture by Thaler et al. [32]. The FBM addresses general behaviour change based on three components: individuals’ motivation, ability and triggers to change behaviour [30]. While Fogg argues that all three components need to be addressed at the same time to

enable behaviour change [30], the COM-B system of Michie et al. [31] induces behaviour change when at least one of its components is addressed: individuals' capability, opportunity, or motivation to change behaviour. The choice architecture of Thaler et al. [32] shifts the perspective away from individuals changing their own behaviour to shaping individuals' choices from the outside, i.e., by nudges.

Another direction of psychological and theoretical behaviour change models is based on the theory of planned behaviour, the theory of reasoned action, the protection motivation theory or deterrence [33], [34], and often promote the use of fear appeal [35]. The theories of planned behaviour and reasoned action assume that individuals when deciding among behaviours are reasonable, make use of information, and consider its implications, i.e., the consequences and perceived probabilities of success and failure [36], [37]. The theory of reasoned action is derived from the theory of planned behaviour and is applied when the subjective probability of success and the degree of control over internal and external factors reach their maximum [37]. Otherwise, the theory of planned behaviour is applied [37]. Based on this Pfleeger and Caputo argue that *"To encourage users to change their security behaviour, the system must create messages that affect users' intentions; in turn, the intentions are changed by influencing users' attitudes through identification of social norms and behavioural control."* ([36], p.608).

However – if they were considered at all in relation to security behaviour in organisations – these theories were mainly considered in connection with the influence of organisational commitment on employees' intentions to comply with security policies [33], [38], rather than from the perspective of practitioners who have to implement behaviour change among their employees. This often involves considering the knowledge, skills, individual preferences, and practices of individuals and groups in relation to information security management [39]. But, promoting secure behaviour within an organisation is a multi-stage process involving various interest groups [40]. This involves not only the perspective of employees, who ultimately have to apply secure behaviour, but also security and security awareness practitioners in organisations who are responsible for planning behaviour change interventions.

For individuals to successfully change their own behaviour, Prochaska et al. [41], [42] have presented a five-stage framework for psychotherapy. Describing five stages that an individual goes through when they want to change their behaviour: pre-contemplation, contemplation, preparation, action, and maintenance [41], [42]. For this, they proposed ten processes for going through their stages of behaviour change. Some of these overlap with our SBCC stages, including *consciousness-raising*, i.e., helping individuals to become aware of causes, consequences and solutions for their problems [41], [42] (cf. STAGE 2), *countering* combined with *environmental control*, i.e., focusing on replacing the undesirable behaviour with an alternative and explicitly removing or replacing those things that are facilitating/supporting the undesirable behaviour [41] (cf. STAGE 7), and *rewards*, i.e., shifting individuals' focus



Fig. 1. The nine-stage behaviour change curve.

towards the prize versus the undesired action [41] (cf. STAGE 8). In contrast to our SBCC, which is intended for practitioners to help their employees to change towards secure behaviour, Prochaska's framework [41] is not related to security and is suitable for individuals who want to change their own behaviour.

C. Security Behaviour Change Curve

The original seven-stage *maturity awareness curve* was first introduced in 2016 by Beyer et al. [1]. The curve conceptualized the idea of tailoring awareness campaigns to employees needs [1]. The *security behaviour change curve* (SBCC) that we use in this paper (see Fig. 1) consists of nine stages (cf [2]). In this section, we first explain the psychological concepts on which the nine-stage SBCC is based. We then provide an overview of where each of these concepts fits into the SBCC stages.

1) Psychological Basis of the Behaviour Change Curve:

a) **Compliance Budget [29]:** The compliance budget describes the phenomenon that employees will only spend a limited amount of time and effort on security measures, and once that limit is reached, the likelihood of non-compliance increases sharply because they try to protect their primary task performance. Most employees will comply with policies addressing risks they recognise if the effort is worth the perceived risk. Otherwise, employees weigh up the behaviour's efforts and benefits before following it [33], [43], including the impact of potential sanctions on them [29]. When perceived security effort exceeds perceived benefit, this is noted and accumulates over the day, until the compliance threshold is reached; once it is, employees are less likely to comply with security policies [29]. To keep the effort required for secure behaviour low, friction between employees' primary tasks and secondary security tasks should be minimised by applying usability principles [44]. However, tough practitioners are aware that security friction is at the root of non-compliance, they currently lack tools and support to reduce it through low-effort security measures, fewer and simpler policies, or better integration into workflows [28].

b) **Self-Efficacy:** Self-efficacy is the belief that one can successfully perform a behaviour to achieve a desired goal [45]. The strength of employees' self-efficacy influences whether they attempt to cope with certain situations, meaning that perceived self-efficacy influences behavioural choices [45]. In the context of security, individuals with higher self-efficacy have a higher adoption rate of secure tools and behaviours, as well as increased intentions to change towards secure behaviour [46]. Consequently, self-efficacy is a significant predictor of intention to comply, and can have a positive effect on attitudes towards security policies [33].

c) **Intentional Forgetting & Habits:** In 2021, the SBCC was extended by the psychological concept of intentional forgetting [14], which can be described as goal-directed, desired forgetting [47], [48]. This is necessary when old behaviours must be discarded to adopt new ones [49]. Intentional forgetting becomes particularly relevant when the behaviours are habitual. Habits are processes in which a stimulus triggers an impulse to act based on a learned stimulus-response association [8]. Helping employees to develop secure habits is more successful in preventing social engineering, like phishing, compared to one-time interventions like training [50], [51]. The SBCC does not aim for short-term behaviour change, but the long-term formation of secure habits. To achieve this, two kinds of habits must be taken into account when applying the SBCC: (1) pre-existing habits, e.g., from the employee's private life, and (2) the secure goal habits that employees should adopt. To form new habits around a desired behaviour, both repetition [12], [13] and rewards that improve overall behavioural performance [15], [52] are needed.

d) **Rewards & Sanctions:** Behavioural learning through direct experience is largely based on receiving rewards or punishments [53]. Rewards improve behavioural performance [15], [54]. Furthermore, incentives can be used to promote behaviour change leading to improved compliance with security guidelines and processes [55]. Sanctions represent the counterpart to rewards. Organisations are already making use of rewards and sanctions in their awareness campaigns [56]. To enable sanctions, incorrect behaviour must first be defined. For this, fear appeals are not effective [40] because they can backfire by triggering defensive reactions in people with low self-efficacy perceptions [57], which was also shown in the medical context [58]. Shaming employees after a security incident has similar effects, as it leads to avoidance or withdrawal behaviour, and hiding of future mistakes [59], [60]. Therefore, fear appeals and shaming must be avoided.

2) **Nine Stages of the Security Behaviour Change Curve:** The SBCC used in this paper consists of nine stages (see Fig. 1). While all nine stages are important for effective behaviour change, it is also possible to "jump" to specific stages based on pre-existing employee knowledge [61].

STAGE 1: Feasibility of Secure Behaviour: To avoid conflicts with employees' compliance budgets [29], organisations must first check the feasibility of secure behaviour as otherwise, the impracticability will increase non-compliance, which also impacts non-security-related behaviours [62]. Fur-

ther, infeasibility could lead employees to circumvent prescribed measures in a way that fits into their daily work routines, thereby creating a feasible imitation of the actual measure [28], [63], [64]. For example, problems with slow VPN connections can lead to employees transferring files locally to their laptops to work on them and transferring them back at the end of the day [63].

STAGE 2: Security Awareness: Employees must be aware of the need to change towards secure behaviour by understanding why security is important. Effective awareness-raising requires consistent communication across various channels [65], [66] where the benefits of secure behaviour should be emphasised [67]. Practitioners should pay attention to how they communicate security topics [17], [18]; the choice of words and technical language can deter employees or give them an incorrect idea of how security measures help [17], [68]. In contrast, information that is personally relevant to employees' security is best processed by employees via the central route of persuasion (elaboration likelihood model) [36]. And also the identifiable victim effect [69] from behavioural science applied to security implies that employees choose stronger security when negative consequences are not abstract but personal and tangible [36].

STAGE 3: Information about Risks & Motivation to Change: Once, people understood that security is important, they need to be educated on specific risks to motivate behaviour change. As experts tend to give differing security advice [70], organisations should determine which risks and advice will be communicated to employees. Risk communication is an important basis for behaviour change, because it is not sufficient to simply instruct employees to behave in a certain secure manner, as a lack of understanding or scepticism regarding the behaviours' necessity may lead to the behaviour not being adopted [71]. Risk communication enables employees to consider cost-benefit ratios into their behaviour [72]. However, the amount of information and notifications provided should be well-balanced, as employees may have different preferences regarding frequency and communication channels, which can determine whether they receive the information or ignore it [26]. Communication should make it clear to employees that they are trusted and supported in their security decisions (to improve motivation) and also explain to them that security vigilance is "business, not personal" [73].

STAGE 4: Understanding (In)Correct Behaviour: Employees should be taught about correct behaviour and how this behaviour protects them from risks communicated earlier [74]. In addition, they should also specifically be taught about incorrect behaviour so that they do not unconsciously adopt it by observing colleagues who behave incorrect [53].

STAGE 5: Agreement through Co-Design: Concordance means that employees agree with the need for behaviour change by committing to implement new behaviour [29]. Changing intentions alone is insufficient [12] because intentions can only determine future behaviour when habits are weak or not yet present [75], since the context that triggers habits is more important than associated goals [76].

In addition, concordance among employees can be achieved through co-design with security practitioners [77] where the common goal is to eliminate friction between the new secure behaviour and the primary tasks of employees. The concept of shadow security [63], [64] (cf. STAGE 1) has shown that employees adopt secure behaviour when they can co-design behaviours that are compatible with their primary tasks.

STAGE 6: Self-Efficacy through Successful Trial & Error: The successful trial and observation of secure behaviour can promote self-efficacy among employees [45], [53]. It is also beneficial if employees feel safe reporting mistakes in the workplace [78]. This reduces stress in relation to secure behaviour and future mistakes can be avoided through vicarious learning [53], [79].

STAGE 7: Environmental Redesign: To break existing habits, the SBCC takes advantage of environmental changes that eliminate habit triggers [12] and foster intentional forgetting [80], [81]. The working environment should be redesigned to promote secure behaviour and prevent insecure behaviour. Secure behaviour should be the first and easiest option. In addition, such environmental or contextual changes can contribute to the favourability of employees' intentions to change their behaviour [12].

STAGE 8: Embedding in Everyday Work: Secure habits must be established by repeating the new secure behaviour many times [12], [13]. Organisations should encourage employees who demonstrate secure behaviour through rewards and recognition [15], [52], [53]. Such compelling incentives combined with an environmental redesign help to overcome status quo bias [36]. Reminders should be context-specific.

STAGE 9: Secure Behaviour is Habit: Once, secure behaviour has become habitual, organisations should continue to visibly recognise and reward secure behaviour [15], [52], [53]. Deliberate refusal to behave securely can be sanctioned from this point onward [53], as it can be assumed that employees who have already adopted secure behaviour no longer have any reason to violate security, unless they do so with malicious intent [73].

III. METHOD

To answer our RQ, we conducted nine workshops with N=25 security and security awareness practitioners that proposed hypothetical plans for applying the SBCC in their organisations to real-world problems.

As a first step to validate the applicability of behaviour change models, Pfleeger and Caputo propose conducting workshops with practitioners and researchers [36]. We opted for a workshop format co-located with a conference for security and security awareness practitioners to attract a big sample that represents the SBCC target group.

A. Participants & Recruitment

Twenty-five security and security awareness practitioners took part in the workshops. Of these, 13 self-identified as female, eleven as male and one as non-binary. The professional experience of our participants varied between 1-3 years (N=8),

TABLE I
DETAILED DEMOGRAPHICS

ID	Age	Gender	Industry sector	S&P Job Experience
P1	25-29 years	f	Retail	1-3 years
P2	35-39 years	f	Food retail	1-3 years
P3	50-54 years	m	Telecommunication	5-10 years
P4	45-49 years	m	NA	over 10 years
P5	40-44 years	f	Military	1-3 years
P6	25-29 years	f	IT services	1-3 years
P7	30-34 years	nb	IT governance	1-3 years
P8	30-34 years	f	Insurance	3-5 years
P9	30-34 years	f	Healthcare	5-10 years
P10	30-34 years	f	Banking	1-3 years
P11	60-64 years	m	University	3-5 years
P12	40-44 years	m	Cultural	over 10 years
P13	40-44 years	m	Consulting	over 10 years
P14	65+ years	m	Telecommunication	over 10 years
P15	35-39 years	f	Security printing	5-10 years
P16	45-49 years	f	University	over 10 years
P17	35-39 years	m	Adult education	5-10 years
P18	40-44 years	f	Telecommunication	1-3 years
P19	45-49 years	m	Finanz	5-10 years
P20	45-49 years	f	Healthcare	5-10 years
P21	25-29 years	m	Energy	3-5 years
P22	35-39 years	f	Consulting	1-3 years
P23	30-34 years	m	Telecommunication	3-5 years
P24	40-44 years	f	Telecommunication	5-10 years
P25	45-49 years	m	Military	over 10 years

3-5 years (N=4), 5-10 years (N=7) and over 10 years (N=6). The practitioners came from diverse industries, ranging from healthcare to retail and banking to the military. All participants hold leading roles in security and security awareness. In *Table I* we report our participants' detailed demographics.

B. Study Procedure

The workshops (approx. 1h) were structured as follows:

a) *Welcome & Consent:* First, participants were briefed and informed about their participant rights, the data collected, and the possibility of withdrawing from the study at any time without negative consequences. This and other information was provided to them via an information sheet, which included a consent form for participants to read and sign. Participants' questions were answered during this process.

b) *Presentation of the Security Behaviour Change Curve:* At the beginning of each workshop the SBCC was presented and the individual stages were explained, to ensure that all participants had a consistent understanding of the SBCC.

c) *Workshops:* The participants applied the SBCC to a self-selected insecure behaviour based on guiding questions (see *Appx. A*) that helped them propose hypothetical behaviour change interventions for all nine SBCC stages. For each SBCC stage, the participants were provided with one paper sheet to write down their considerations.

d) *Demographics:* Finally, participants completed demographic questionnaires and were thanked for participation.

Piloting: The presentation and SBCC description were feedbacked by five experts from the fields of psychology and security. Based on this, we revised the presentation to improve clarity. We then conducted a pilot workshop with three participants with a background in psychology and security to ensure that our guiding questions were clear and understandable. The pilot workshop enabled us to make final adjustments to our

guiding questions. However, data from the pilot workshop is not included in the results presented in this paper.

C. Data Analysis

Before the analysis, we first anonymised all collected data. To ensure that participants could not be identified by their handwriting on the paper sheets, these were digitised. Two researchers then independently analysed the workshop artefacts through qualitative analysis based on Kuckartz [82]. First, we performed inductive open coding. One researcher familiar with the data created an initial code book. The code book was then reviewed by a second researcher who was present during the workshops and had also familiarised themselves with the data. The codebook was then applied to all collected data by the first researcher and verified by the second one. Disagreements were resolved through discussion. The workshop artefacts were finally clustered to the SBCC stages.

D. Limitations

Like most qualitative studies, our work is subject to limitations that must be considered when reading our results. First, our study is based on self-reported data, which might be biased due to social desirability, availability bias, and wrong recalls. Consequently, our data only reflects the highly subjective views of our participants. Second, while we recruited a diverse set of security and security awareness practitioners from different kinds of organisations, they might not be representative of the overall population of security and security awareness practitioners. Third, our workshops were limited to one hour, naturally limiting the depth of participants' discussions. Finally, we present the first evaluation of the SBCC with the target group. Although we prompted our participants to consider and answer the guiding questions as they would in their work setting, their planned interventions remain hypothetical. Consequently, our results need to be extended and confirmed by long-term studies applying the SBCC in organisations including pre-/post assessments.

E. Ethical Considerations

Our local regulations do not require an ERB/IRB for the study that we conducted. Yet, we took precautions to treat our participants in an ethically correct manner by adhering to the Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct [83], the Ethical Principles of Psychologists and the Code of Conduct of the American Psychological Association [84], as well as the Declaration of Helsinki [85]. Further, we followed strict national privacy laws: Participants received a consent form with detailed information about the captured data, that participants could at any point abort participating without negative consequences, and information about participants' rights compliant with the GDPR and national data protection laws. As participants took part in the co-located conference, the workshops were a voluntary part of the conference program.

IV. FINDINGS

In this section, we present the results of the nine workshops, some of them with specific reference to the respective behaviour under consideration, others in general terms, as they can be applied to any security behaviour. Here, N represents the number of workshop groups that addressed a particular topic or made a statement, and G represents the specific group.

A. Current Problematic Behaviour in Organisations

Before specifically working with the SBCC, we asked participants to provide problematic behaviours they recently observed in their work context. Overall, our participants identified 32 of such behaviours and suggested 25 more secure solutions. The considered behaviours centred around employees handling:

- **Physical Access** ($N=6$): “Employees should have a neutral key ring so that access tokens cannot be easily assigned by outsiders.” ($G2$),
- **Data and Information** ($N=7$): “Sensitive data should not be shared on social media; conscious use of social media is necessary.” ($G5$),
- **Accounts** ($N=5$): “Passwords should not be reused. One service = one password.” ($G6$),
- **Hardware** ($N=7$): “Unknown USB sticks should be handed in to IT.” ($G9$),
- **Software** ($N=2$): “Set up technical security measures.” ($G1$), and
- **Incidents** ($N=4$): “Open an incident with the helpdesk, call the helpdesk number” ($G7$),

as well as the general circumvention of security measures and company policies.

Next, each group was asked to focus on one behaviour and analyse it in detail. The analysed behaviours were: (1) LOCKING DEVICES when left behind ($G1$ & $G8$), (2) PHYSICAL ACCESS CONTROL to buildings and how it is handled ($G2$ & $G3$), (3) INCIDENT & PHISHING REPORTING by employees ($G4$ & $G7$), (4) PASSWORD REUSE ($G5$ & $G6$), and (5) USING USB-STICKS that were found ($G9$). All but one (using USB-sticks) of the five behaviours were considered at least in two workshops. Therefore, the remaining findings focus on the first four behaviours mentioned.

B. STAGE 1: Feasibility of Secure Behaviour

Our participants identified several potential conflicts of their chosen security behaviour with employees' primary tasks that prevent employees from adopting secure behaviour. These conflicts can be grouped into conflicts and workarounds that (a) apply generally to the formation of secure behaviour, and that (b) only apply to specific behaviours.

a) *General Conflicts & Workarounds*: General conflicts can be of a personal ($N=9$) or structural ($N=12$) nature. Personal conflicts – taking place at the emotional level of employees – identified by our participants included: shame, fear, a feeling of powerlessness and laziness. Structural conflicts – stemming from the corporate culture – can be influenced by hierarchies, error culture and time management, as discussed

by our participants. Overall, perceived time loss was the conflict most frequently discussed ($N=7$). Our participants named two general workarounds to avoid the use of tools or secure behaviours prescribed by company policies: (1) ignoring the prescribed measures and (2) the collective solidarity of employees in their insecure behaviour.

b) Behaviour-bound Conflicts & Workarounds: In addition to the general conflicts and workarounds, our participants also identified many that occur primarily in connection with the behaviours they discussed, except for USING USB-STICKS. For the behaviour-bound conflicts and workarounds see *Table II, Col. 2*.

C. STAGE 2: Security Awareness

Employees must be made aware of the importance of secure behaviour and that the advantages of secure behaviour should be emphasized.

a) Current Security Awareness Measures: In this context, our participants listed 40 different awareness-raising measures that are currently implemented in their organisations (see *Tab. III*). These can be sub-divided into 22 active and 18 passive measures. Active measures involve the active participation of employees or require them to take action to acquire skills and knowledge; training courses are a common example for this. In passive measures, employees receive information without actively participating, e.g., by posters or videos.

b) Advantages of Secure Behaviour: In addition to the methods currently used to increase security awareness, our participants discussed the specific behaviour advantages and how these could be highlighted (see *Tab. II, Col. 3*). While each secure behaviour has its own advantages, our participants also identified some general ones. These are mainly personal advantages for employees, such as improved security awareness and the acquisition of competences, combined with the transfer of the secure behaviour to their private lives.

D. STAGE 3: Information about Risks & Motivation to Change

Detailed information about risks and consequences should be made available to employees. To help employees understand the big picture – how data and information are used by attackers – our participants have identified specific attackers and their targets based on the insecure behaviour they worked on during the workshop (see *Tab. II, Col. 4*).

While the type of attacker may vary depending on the insecure behaviour, the attackers' objectives in the corporate context identified by our participants are similar, and can be divided into two categories: data ($N=7$) and infrastructure ($N=8$). With data as the attack target, practitioners say it is not just a matter of data theft ($N=2$), but also manipulation ($N=2$), and deletion ($N=1$). In the case of attacks on the organisation's infrastructure, practitioners saw it particularly problematic that attackers could gain system access to company applications ($N=5$), emails ($N=1$), and social media accounts ($N=1$). These attacks usually attempt to remain undetected in the system for as long as possible ($N=2$).

The targets and effects of attacks are also closely linked to the services provided by the various companies. During the workshop, one participant noted that in hospitals it is difficult to identify attackers on PHYSICAL ACCESS CONTROL as such, as there are also many legitimate visitors and patients. Thus, it can already be considered an attack when outsiders interfere with operational processes ($N=1$). However, intentional sabotage can also occur in this area ($N=1$).

E. STAGE 4: Understanding Correct & Incorrect Behaviour.

To provide employees with knowledge about secure behaviour, how the behaviour protects against risks, and incorrect behaviour, our participants developed clear Dos and Don'ts (see *Tab. II, Col. 5*).

F. STAGE 5: Agreement through Co-Design

Employees must agree to the secure behaviour, actively committing to the objectives and agree on their achievability. Our practitioners developed opportunities for employees to raise questions and concerns and have a stake in how behaviours are implemented.

The suggestions on how employees can raise questions and concerns can be divided into DIGITAL, mostly asynchronous communication channels and ANALOGUE, synchronous communication channels. For digital, asynchronous channels, ticket systems ($N=2$), emails ($N=1$) and community platforms, such as intranet portals ($N=2$), were suggested. However, some digital channels, depending on their implementation, also enable synchronous communication, e.g., helpdesks ($N=4$) or chatbots ($N=1$). All suggested analogue channels require direct synchronous exchanges in Q&A sessions ($N=1$) or with a corresponding contact person ($N=3$).

The co-design opportunities for employees suggested by our participants can be divided into PASSIVE, more asynchronous and ACTIVE co-design. The passive options include internal platforms ($N=5$), e.g., intranet forums. For the active options, our practitioners suggested continuous co-design processes to be established ($N=6$) that involve employees in the introduction of new secure behaviours from the outset. More specific examples were the organisation of interdisciplinary workshops and focus groups ($N=4$), surveys ($N=2$), and training of employees as multipliers ($N=1$).

G. STAGE 6: Self-Efficacy through Successful Trial & Error

As employees need to gain confidence in their own abilities to adopt new behaviour, we asked our practitioners how to enable employees to try out or observe secure behaviour. Furthermore, the focus was on avoiding fear and failure among employees. In addition to well-known methods, such as simulated attacks ($N=5$), the practitioners suggested less established trial opportunities for employees.

One of these suggested trial opportunities are so-called F***-up Nights ($N=5$) where employees learn security-related behaviour, try it out, train, and watch demos of the effects of a successful attack in a safe environment in which no judgement is made and no actual damage is done in the event of mistakes.

TABLE II
BEHAVIOUR-BOUND RESULTS

Behaviour	STAGE 1 Conflicts & Workarounds	STAGE 2 Advantages	STAGE 3 Attackers	STAGE 4 Dos & Don'ts	STAGE 7 Trigger & Redesign
LOCKING DEVICES (G1 & G8)	Conflicts: Time loss, annoyance, forgetting, justifying exceptions. Workarounds: Running active software sessions. Playing videos. Using keyboard simulators. Extending the time before the auto screensaver. Requesting admin rights to change locking settings.	Protects devices from physical access by third parties	Individuals who gained unauthorized physical access. Insider attackers.	Dos: "Lock devices as soon as you move out of sight, e.g., using the keyboard combination [Win + L]." Don'ts: "Leaving devices unlocked when unattended."	Redesign: Placing signs or Post-it notes on employee devices.
PHYSICAL ACCESS CONTROL (G2 & G3)	Conflicts: On an interpersonal level, willingness to help, time loss. Workarounds: Tailgating.	Protection of devices, work equipment, and data. Valuable for the organisation in terms of certification evidence and an positive impression on customers. Employees gain more self-confidence in interpersonal interactions.	Individuals who gained unauthorized physical access. Tradespeople. Counterfeiters.	Dos: "Close doors. Question unauthorised persons. Management should function as a role model." Don'ts: "Leaving doors open. Manipulating locking mechanisms. Let unknown people in. Do not underestimate the risks."	Trigger: Conflicts with people who actually have access authorisation, or even punishment despite correct behaviour. Redesign: Eliminate wedging possibilities. Install automatic door closers (with alarms). Physical security checks by a person. Clearly visible employee badges.
INCIDENT & PHISHING REPORTING (G4 & G7)	Conflicts: Cumbersome reporting process, fear of embarrassment, not feeling responsible. Workarounds: Covering up incidents, lying.	Shorter response time. Less impactful attacks. Lower probability of attacks. Rapid prevention of attacks	Social engineering by state actors, industrial spies, hackers.	Dos: "Report incidents, no matter how small they appear. Be willing to put in the effort. Take responsibility." Don'ts: "Looking away or ignoring incidents."	Trigger: Unclear reporting processes. (Neg.) Reaction to reporting of self-inflicted incidents. Redesign: New reporting interface, single reporting location, simple reporting button. Anchor reporting in work values (annual targets, positive feedback, role modelling).
PASSWORD REUSE (G5 & G6)	Conflicts: Setup of password managers (PWMs) and creation of unique passwords for existing accounts (time loss), impracticability of device-bound PWMs when using multiple devices (outside the organisation). Workarounds: Setting up or having pre-installed PWMs, but not using them.	Reduced mental strain. Better protected, e.g., against identity theft	Colleagues. Family members.	Dos: "Create a new password for each new service. Set up a PWM with one complex master password. Separate business and private accounts." Don'ts: "Reusing passwords for several services. Using a simple master password. Sharing passwords."	Trigger: Needing updates, malfunctions, lack of device support, different password requirements. Lack of clarity, feeling stressed, overwhelmed, (in)convenience. Redesign: Pre-installed PWMs with obligation to use, automatic filling of password fields, suggesting strong passwords. Offering family licences, enabling employees to use the same PWMs on private devices.

TABLE III
SECURITY AWARENESS MEASURES CURRENTLY IMPLEMENTED IN PARTICIPANTS' ORGANISATIONS

Current Active Security Awareness Measures		N
Target group-specific	On-site training	4
	Hackathons	1
	Gamification	2
Individual	E-learning courses	9
	Phishing simulations	1
Group-based	Tabletop games	1
	Escape rooms	2
	Workshops	2
Current Passive Security Awareness Measures		N
Company guidelines	Branding	1
	Policies	1
	Onboarding processes	1
		1
Presentations	Roadshows	1
	On-site lectures	1
	Live hacking	2
Analogue materials	Flyers, posters, comics, ...	7
Digital materials	Videos, intranet posts, ...	4

Other suggestions included increasing self-efficacy through social learning ($N=3$), i.e. consciously modelling secure behaviour through role models and observation. With specific reference to PASSWORD REUSE, the groups suggested that employees could volunteer to participate in pilot groups to test the introduction of password managers. Such pilot projects can also be generalised for the introduction of new tools. Our participants also became more specific with regard to INCI-

DENT AND PHISHING REPORTING, suggesting that employees should send a test report via the reporting system, followed by feedback to familiarise with the process.

To avoid failure and fear, practitioners have identified various aspects that need to be taken into account. These include starting slowly and gradually introducing new behaviours by providing tools and guidance and recognising small successes. In addition, an open culture of error management should be practised, which means that contact points and reporting centres should also be trained accordingly.

H. STAGE 7: Environmental Redesign

We asked our practitioners how working environments can be redesigned with the aim of preventing insecure behaviour by making secure behaviour the first and simplest option.

For this, participants first identified trigger for the old insecure behaviour (see *Tab. II, Col. 6*). With regard to PASSWORD REUSE, our participants identified tool-based and emotional triggers. While tool-based triggers vary depending on the behaviour and tool in question, emotional triggers depend on the individual. The triggers our participants saw for employees continuing to use FOUND USB-STICKS are that the corresponding computer ports are not deactivated.

Based on the identified trigger, our participants came up with suggestions on how to redesign the working environment. To prevent employees from using unknown hardware, such

as FOUND USB-STICKS, ports should be restricted and other alternatives for sharing data introduced instead. Easy access to service points where employees can hand in unknown and found hardware and receive advice should also be provided.

I. STAGE 8: Embedding in Everyday Work

Once triggers have been eliminated and secure behaviour has become the easiest option, employees must develop habits. For this, organisations should encourage employees who demonstrate secure behaviour by rewards and recognition.

a) Habituation: As a first step toward habituation, our participants suggested that onboarding should take place during team meetings and that regular reminders should be provided. In the case of newly introduced security tools, they further suggested that regular provision of information about new features should serve as a reminder to use the new tool and help users adapt to it. As further forms of conditioning, our participants considered conducting exercises ($N=2$), introducing reward systems ($N=3$), modelling safe behaviour, and also psychological concepts such as nudging or gamification in the form of competitions ($N=3$).

b) (Short-Term) Rewards: To reward secure behaviour, our participants discussed three reward types: MATERIAL ($N=7$), INTERPERSONAL ($N=6$), and in the form of CAREER OPPORTUNITIES ($N=2$). MATERIAL rewards mainly involved prizes and awards in competitions as known from other industry domains. Specific examples included stickers or mouse pads as security merchandise. INTERPERSONAL appreciation our participants considered to take the form of public or visible recognition, but also positive feedback and integration into groups. Suggested CAREER OPPORTUNITIES included special support or preferential treatment with regard to promotions.

More concrete suggestions were: getting chocolate for LOCKING DEVICES, a reward if no alarm is triggered during PHYSICAL ACCESS CONTROL, positive feedback and recognition in post-INCIDENT communication, and rewarding the number of unique PWM entries to avoid PASSWORD REUSE.

J. STAGE 9: Secure Behaviour is Habit

Once secure behaviour is habitual, organisations should continue to visibly recognize and reward secure behaviour. Deliberate refusal to engage in secure behaviour can be sanctioned from this point on.

a) (Long-Term) Rewards: The long-term rewards suggested by our participants can be categorized into the same three reward types as short-term rewards: MATERIAL ($N=6$), INTERPERSONAL ($N=5$), and CAREER OPPORTUNITIES ($N=3$). As long-term MATERIAL rewards, our participants suggested collectibles, such as badges, trophies, and awards, but also again security merchandise. Long-term INTERPERSONAL rewards should continue to consist of visible recognition of correct secure behaviour and celebration of small successes. However, our participants also suggested running leader-boards as a long-term incentive and reward in one. As long-term CAREER OPPORTUNITIES, our participants suggested bonuses that are set out in target agreements.

b) Refusal to Behave Securely & Sanctions: To determine which behaviour should be sanctioned, it must be established what constitutes a refusal to behave securely. On the one hand, our participants mentioned general refusals, such as compliance violations or indifference to company policies. On the other hand, they named specific violations related to the behaviour they investigated: The use of presence simulation tools to circumvent LOCKING DEVICES, the sabotage of closing mechanisms for PHYSICAL ACCESS CONTROL, failure to use a mandatory PASSWORD MANAGER, failure to hand in, or leaving UNKNOWN HARDWARE lying around and its use.

As specific sanctions for NOT LOCKING DEVICES, our participants suggested adjusting screen settings and sending invitations to eat home-made cake. Another suggestion was the internal publication of hacked passwords in the event of PASSWORD REUSE. Overall, our participants further suggested to arrange sanctions in an escalation process: 1) Warning, 2) Personal meeting, 3) Withdrawal of benefits, 4) No promotion, 5) Management-imposed requirements, 6) Termination.

V. DISCUSSION

In our workshops, security and security awareness practitioners applied the SBCC to specific, self-selected, insecure behaviours that they had observed in their work context. While all practitioners were able to use the SBCC without problems, the evaluation of the scenarios revealed approaches taken by practitioners that are outdated from a human-centred security perspective. In the following, we will address these points to enable practitioners to apply the SBCC more easily and effectively.

A. Implications for Practitioners based on the Workshops

As seen by the example of potential attackers targeting unlocked devices and insufficient physical access control, insecure behaviours and associated attacks can influence each other. Practitioners can take advantage of this by emphasizing the importance of secure behaviour based on other insecure behaviours and the shift of attacks towards them.

a) Interventions must be done in the correct stage: It is essential to link interventions to the most suitable SBCC stage to be effective. Wrongly placed interventions might backfire [6]. Simulated attacks are a well-known representative for this: Although the literature has repeatedly shown that they, especially in the context of anti-phishing trainings, are counter-productive for the self-efficacy of employees [5], [6], [25], five out of the nine practitioner groups suggested this as a trial opportunity to introduce employees to secure behaviour. Here, an essential distinction has to be made: exposing employees to veiled attack simulations without further support and information to ‘test’ them is less effective. However, simulations can be viable opportunities for employees to experience the effects of attacks in a secure environment (see STAGE 6). Yet they should not be used in earlier stages, for instance to motivate employees (STAGE 3), or later ones to sanction them (STAGE 9).

b) Consideration of resources: In order to avoid overwhelming employees with regard to their compliance budget [29] when introducing new tools, as in the case of password managers to prevent PASSWORD REUSE, the organisation's resources should be considered. In most cases, not only are one-off acquisition costs required, but the tools also need to be serviced and maintained on employees' devices. If employees are left to do this by themselves, friction arises that hinders the habit formation necessary for long-term behavioural change.

c) Employees need concrete but not too technical knowledge: We observed that the list of attackers mentioned by our participants was not exhaustive, and broad terms, such as "everyone" or "hackers", without specifying them further were used. While this can be acceptable among experts, as they can imagine various possible attackers, it is necessary to be more specific when communicating with non-experts. Employees without advanced security knowledge often cannot imagine which attackers are meant by generic terms leading to wrong risk assessments [86].

d) Short-term vs. long-term rewards: Our participants had difficulties distinguishing between short- and long-term rewards, with their suggestions overlapping for both (cf. Sect. IV-10b & IV-10a). Here, a distinction should be made between short-term rewards for employees to form habits and long-term rewards to maintain them. Especially short-term rewards are needed in large quantities at the beginning. After that, the number and timing of rewards can be adjusted, e.g., according to the hook model [87]. Once employees have formed habits, organisations can transition to long-term rewards. However, organisations should never remove short-term rewards, as these continue to provide motivational peaks [87].

B. Additional guidance for Practitioners on using the SBCC

During the workshops, we noticed open questions regarding the application of the SBCC that we would like to address here.

a) Sanctions should be considered carefully: For most employees, depending on their roles, security is a secondary task. Nevertheless, there are security behaviours that every employee should practice in general. Here, the goal should not be to train every employee to become security experts, but rather to encourage certain behaviours to become habitual so that employees are not distracted from their actual tasks. Therefore, care should be taken when deciding which behaviours to sanction. If direct and deliberate compliance violations occur after secure behaviour has become habitual, these can be sanctioned. However, unintentional violations such as accidentally clicking on a phishing email should not be sanctioned, as this fear appeal will only lead to employees concealing similar incidents in the future [59], [60].

b) Individuality in habit formation must be respected: Even if behavioural change interventions are planned using the SBCC, real behavioural change ultimately happens within individual employees. Therefore, it should not be assumed that a one-size-fits-all development process will be observed when intervention planning is applied. An employee-centred

management style is needed. On the one hand, habit formation differs among individuals [13]. On the other hand, personal factors and characteristics of employees, as observed in the triggers, also play a role. For example, a longer absence of employees because of holidays or illness can interrupt their habit formation due to a lack of consistency [13], [88].

C. Guidance for Future Research

While the workshops showed that security and security awareness practitioners can apply the nine SBCC stages to ideate interventions, we have not examined the implementation of interventions in organisations with employees. Hence, the question of whether interventions developed using the SBCC are effective in bringing about behavioural change remains open even though the theoretical framework has been developed to specifically enable this. Future work should extend our results by long-term investigations by applying the SBCC in organisations including pre-/post assessments.

First, large scale investigations should collect real-world data on insecure behaviour that requires behaviour change. Here, it is crucial to consider different populations and cultures, as these influence insecure behaviour and the resulting interventions should be tailored accordingly. Once such a basis is established, the SBCC should be applied to collect best practice interventions by fostering exchange between practitioners and academia, again considering different populations and cultures. Fostering exchange is essential, as practitioners might use outdated interventions as our results show. Field and in-the-wild studies should investigate the long-term efficacy of individual methods. Further future work should investigate how to best communicate the theoretical framework to practitioners ultimately moving beyond current practices of conducting security training to "tick" compliance boxes, towards long-term commitments for secure behaviour in organisations. Here, specifically adapting the SBCC with CEOs as target groups might be a valuable starting point for future work.

Finally, since employees might "bring" security habits from home to work, using parts of the SBCC in early education, e.g., in schools, might be a viable solution to mitigate insecure behaviour in the first place. For this, future work should adapt the SBCC from the professional to private contexts.

VI. CONCLUSION

In this paper, we investigated whether security and security awareness practitioners can apply the theoretically grounded SBCC [1], [14]. Therefore, we conducted nine workshops with a total of N=25 practitioners. The workshops' results showed that practitioners can use the theoretical SBCC to ideate interventions that promote behaviour change among employees towards secure behaviour. However, when considering our participants' suggestions, we identified some persistent problems with current awareness-raising measures, which are already outdated and have been challenged by research findings. The aim of this work was not only to test the applicability of the SBCC by practitioners, but also to unravel the psychological concepts underlying the SBCC for practitioners. To this end,

in addition to breaking down the SBCC, we also present extended guiding questions that practitioners can use along the SBCC to plan interventions. Future work should investigate the effectiveness of interventions designed based on the SBCC in real-world settings. For this, long-term field studies in collaboration with organisations are required.

ACKNOWLEDGMENTS

We thank all participants in our study. This work was co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972 and the BMFTR (Federal Ministry for Research, Technology and Space) as of the project grant number 16KIS1646K: DigiFit (Digital fitness for citizens - realistic risk perceptions, secure routines).

REFERENCES

- [1] M. Beyer, S. Ahmed, K. Doerlemann, S. Arnell, S. Parkin, A. Sasse, and N. Passingham, "Awareness is only the first step: A framework for progressive engagement of staff in cyber security," *Hewlett Packard, Business white paper*, 2016, [Accessed: July 24, 2026]. [Online]. Available: <https://www.slideshare.net/slideshow/awareness-is-only-the-first-step/55894537>
- [2] M. A. Sasse, J. Hielscher, J. Friedauer, and A. Buckmann, "Rebooting it security awareness – how organisations can encourage and sustain secure behaviours," in *Computer Security. ESORICS 2022 International Workshops*. Cham: Springer International Publishing, 2023, pp. 248–265, [Accessed: July 30, 2026]. [Online]. Available: https://doi.org/10.1007/978-3-031-25460-4_14
- [3] N. Sebescen and J. Vitak, "Securing the human: Employee security vulnerability risk in organizational settings," *Journal of the Association for Information Science and Technology*, vol. 68, no. 9, pp. 2237–2247, 2017, [Accessed: July 24, 2026]. [Online]. Available: <https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.23851>
- [4] J. Hielscher and M. Golla, "Quantifying security training in organizations through the analysis of u.s. sec 10-k filings," in *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '25. New York, NY, USA: Association for Computing Machinery, 2025, p. 51–65, [Accessed: July 24, 2026]. [Online]. Available: <https://doi.org/10.1145/3719027.3765179>
- [5] D. Lain, K. Kostianen, and S. Čapkun, "Phishing in organizations: Findings from a large-scale and long-term study," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 842–859, [Accessed: July 24, 2026]. [Online]. Available: <https://ieeexplore.ieee.org/abstract/document/9833766>
- [6] G. Ho, A. Mirian, E. Luo, K. Tong, E. Lee, L. Liu, C. A. Longhurst, C. Dameff, S. Savage, and G. M. Voelker, "Understanding the efficacy of phishing training in practice," in *2025 IEEE Symposium on Security and Privacy (SP)*, 2025, pp. 37–54, [Accessed: July 24, 2026]. [Online]. Available: <https://ieeexplore.ieee.org/document/11023357>
- [7] L. Brunken, A. Buckmann, J. Hielscher, and M. A. Sasse, "“To do this properly, you need more Resources”: The hidden costs of introducing simulated phishing campaigns," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 4105–4122, [Accessed: July 24, 2026]. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity23/presentation/brunken>
- [8] B. Gardner, "A review and analysis of the use of ‘habit’ in understanding, predicting and influencing health-related behaviour," *Health Psychology Review*, vol. 9, no. 3, pp. 277–295, 2015, [Accessed: July 24, 2026]. [Online]. Available: <https://doi.org/10.1080/17437199.2013.876238>
- [9] L. Carden and W. Wood, "Habit formation and change," *Current Opinion in Behavioral Sciences*, vol. 20, pp. 117–122, 2018, [Accessed: July 24, 2026]. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2352154617301602>
- [10] L. Ordóñez and L. Benson, "Decisions under time pressure: How time constraint affects risky decision making," *Organizational Behavior and Human Decision Processes*, vol. 71, no. 2, pp. 121–140, 1997, [Accessed: July 24, 2026]. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0749597897927175>
- [11] A. Musarurwa, S. Flowerday, and L. Cilliers, "The bring-your-own-device unintended administrator: A perspective from zimbabwe," *THE ELECTRONIC JOURNAL OF INFORMATION SYSTEMS IN DEVELOPING COUNTRIES*, vol. 85, no. 4, 2019, [Accessed: July 27, 2026]. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/isd2.12076>
- [12] W. Wood, L. Tam, and M. G. Witt, "Changing circumstances, disrupting habits," *Journal of personality and social psychology*, vol. 88, no. 6, p. 918, 2005, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1037/0022-3514.88.6.918>
- [13] P. Lally, C. H. M. van Jaarsveld, H. W. W. Potts, and J. Wardle, "How are habits formed: Modelling habit formation in the real world," *European Journal of Social Psychology*, vol. 40, no. 6, pp. 998–1009, 2010, [Accessed: July 27, 2026]. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/ejsp.674>
- [14] J. Hielscher, A. Kluge, U. Menges, and M. A. Sasse, "“Taking out the Trash”: Why security behavior change requires intentional forgetting," in *Proceedings of the 2021 New Security Paradigms Workshop*, ser. NSPW '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 108–122, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3498891.3498902>
- [15] R. M. Krebs, C. N. Boehler, and M. G. Woldorff, "The influence of reward associations on conflict processing in the stroop task," *Cognition*, vol. 117, no. 3, pp. 341–347, 2010, [Accessed: July 27, 2026]. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0010027710001988>
- [16] G. Judah, B. Gardner, M. G. Kenward, B. DeStavola, and R. Aunger, "Exploratory study of the impact of perceived reward on habit formation," *BMC psychology*, vol. 6, no. 1, p. 62, 2018, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1186/s40359-018-0270-z>
- [17] L. C. Neil, C. Healy, and J. Haney, "“A five-year-old could understand it” versus “This is way too confusing”: Exploring non-expert understandings and perceptions of cybersecurity definitions," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, ser. CHI '25. New York, NY, USA: Association for Computing Machinery, 2025, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3706598.3713820>
- [18] F. Meissner, J. M. Nold, M. A. Sasse, R. Pankus, and A. Wilke, *Uncertain Journeys into Digital Futures*, 1st ed., ser. Normsetzung und Entscheidungsverfahren – Schriftenreihe des Weizenbaum-Instituts für normative Wissenschaften. Baden-Baden: Nomos, 2025, vol. 1, ch. "Encryption doesn't matter": Pitfalls in cybersecurity communications, pp. 219–238, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.5771/9783748947585-219>
- [19] A. Buckmann, J. M. Nold, Y. Acar, and Y. Zou, "More than usability: Differential access to digital security and privacy," in *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*. Seattle, WA: USENIX Association, Aug. 2025, pp. 455–474, [Accessed: July 30, 2026]. [Online]. Available: <https://www.usenix.org/conference/soups2025/presentation/buckmann>
- [20] J. Hielscher, M. Schöps, J. Opdenbusch, F. Reichmann, M. Gutfleisch, K. Marky, and S. Parkin, "Selling satisfaction: A qualitative analysis of cybersecurity awareness vendors' promises," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 2666–2680, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3658644.3690196>
- [21] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, Jun. 2010, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/1754393.1754396>
- [22] J. Hielscher, U. Menges, S. Parkin, A. Kluge, and M. A. Sasse, "“Employees who Don't accept the time security takes are not aware Enough”: The CISO view of Human-Centred security," in *32nd USENIX Security Symposium (USENIX Security 23)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 2311–2328, [Accessed: July 27, 2026]. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher>

- [23] M. Schöps, M. Gutfleisch, E. Wolter, and M. A. Sasse, "Simulated stress: A case study of the effects of a simulated phishing campaign on employees' perception, stress and Self-Efficacy," in *33rd USENIX Security Symposium (USENIX Security 24)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 4589–4606, [Accessed: July 27, 2026]. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity24/presentation/sch%C3%B6ps>
- [24] K. Schiller, F. Adamsky, C. Eichenmüller, M. Reimert, and Z. Benenson, "Employees' attitudes towards phishing simulations: "It's like when a child reaches onto the hot hob"," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 4167–4181, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3658644.3690212>
- [25] M. Volkamer, M. A. Sasse, and F. Boehm, "Analysing simulated phishing campaigns for staff," in *Computer Security. ESORICS 2020*, I. Boureanu et al., Ed. Cham: Springer International Publishing, 2020, pp. 312–328, [Accessed: July 24, 2026]. [Online]. Available: https://doi.org/10.1007/978-3-030-66504-3_19
- [26] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Security Privacy*, vol. 12, no. 1, pp. 28–38, 2014, [Accessed: July 27, 2026]. [Online]. Available: <https://ieeexplore.ieee.org/document/6585241>
- [27] D. Lain, T. Jost, S. Matetic, K. Kostianen, and S. Capkun, "Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 4182–4196, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3658644.3690348>
- [28] J. Hielscher, M. Schöps, U. Menges, M. Gutfleisch, M. Helbing, and M. A. Sasse, "Lacking the tools and support to fix friction: Results from an interview study with security managers," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 131–150, [Accessed: July 27, 2026]. [Online]. Available: <https://www.usenix.org/conference/soups2023/presentation/hielscher>
- [29] A. Beauteament, M. A. Sasse, and M. Wonham, "The compliance budget: managing security behaviour in organisations," in *Proceedings of the 2008 New Security Paradigms Workshop*, ser. NSPW '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 47–58, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/1595676.1595684>
- [30] B. Fogg, "A behavior model for persuasive design," in *Proceedings of the 4th International Conference on Persuasive Technology*, ser. Persuasive '09. New York, NY, USA: Association for Computing Machinery, 2009, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/1541948.1541999>
- [31] S. Michie, M. M. van Stralen, and R. West, "The behaviour change wheel: A new method for characterising and designing behaviour change interventions," *Implementation Science*, vol. 6, p. 42, 2011, [Accessed: July 31, 2026]. [Online]. Available: <https://doi.org/10.1186/1748-5908-6-42>
- [32] R. H. Thaler, C. R. Sunstein, and J. P. Balz, "Choice architecture," *Harvard Public Law Working Paper Forthcoming*, 2010, [Accessed: July 31, 2026]. [Online]. Available: <http://dx.doi.org/10.2139/ssrn.1583509>
- [33] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2, pp. 106–125, 2009, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1057/ejis.2009.6>
- [34] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers Security*, vol. 31, no. 1, pp. 83–95, 2012, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.cose.2011.10.007>
- [35] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors1," *Management Information Systems Quarterly*, vol. 39, no. 4, pp. 837–864, 12 2015, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.25300/MISQ/2015/39.4.5>
- [36] S. L. Pfleeger and D. D. Caputo, "Leveraging behavioral science to mitigate cyber security risk," *Computers Security*, vol. 31, no. 4, pp. 597–611, 2012, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.cose.2011.12.010>
- [37] I. Ajzen, *From Intentions to Actions: A Theory of Planned Behavior*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39, [Accessed: July 27, 2026]. [Online]. Available: https://doi.org/10.1007/978-3-642-69746-3_2
- [38] R. F. Ali, P. D. D. Dominic, S. E. A. Ali, M. Rehman, and A. Sohail, "Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance," *Applied Sciences*, vol. 11, no. 8, 2021, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.3390/app11083383>
- [39] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: a behaviour compliance conceptual framework," in *Proceedings of the Eighth Australasian Conference on Information Security - Volume 105*, ser. AISC '10. AUS: Australian Computer Society, Inc., 2010, p. 47–55, [Accessed: July 27, 2026]. [Online]. Available: <https://dl.acm.org/doi/10.5555/1862266.1862275>
- [40] European Union Agency for Cybersecurity, *Cybersecurity culture guidelines - Behavioural aspects of cybersecurity*, A. Bourka and P. Drogkaris, Eds. European Network and Information Security Agency, 2018, [Accessed: July 27, 2026]. [Online]. Available: <https://data.europa.eu/doi/10.2824/324042>
- [41] J. Prochaska, J. Norcross, and C. DiClemente, *Changing for Good: A Revolutionary Six-Stage Program for Overcoming Bad Habits and Moving Your Life Positively Forward*. HarperCollins, 2010, [Accessed: July 27, 2026]. [Online]. Available: <https://books.google.de/books?id=ibnlpYe2JggC>
- [42] J. O. Prochaska and C. C. Diclemente, "The transtheoretical approach," in *Handbook of Psychotherapy Integration*, J. C. Norcross and M. R. Goldfried, Eds. Oxford University Press, 02 2005, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1093/med:psych/9780195165791.003.0007>
- [43] P. Todd and I. Benbasat, "The influence of decision aids on choice strategies: An experimental analysis of the role of cognitive effort," *Organizational Behavior and Human Decision Processes*, vol. 60, no. 1, pp. 36–74, 1994, [Accessed: July 27, 2026]. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0749597884710740>
- [44] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal*, vol. 19, no. 3, pp. 122–131, 2001, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1023/A:1011902718709>
- [45] A. Bandura, "Self-efficacy: Toward a unifying theory of behavioral change," *Psychological Review*, vol. 84, no. 2, pp. 191–215, 1977, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1037/0033-295X.84.2.191>
- [46] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers Security*, vol. 28, no. 8, pp. 816–826, 2009, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.cose.2009.05.008>
- [47] E. Bjork, R. Bjork, and M. Anderson, *Intentional forgetting: interdisciplinary approaches*. Lawrence Erlbaum Associates, 01 1998, ch. Varieties of Goal Directed Forgetting, pp. 103–137, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.4324/9780203774434>
- [48] H. M. Johnson, "Processes of successful intentional forgetting," *Psychological Bulletin*, vol. 116, no. 2, p. 274–292, 1994, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1037/0033-2909.116.2.274>
- [49] E. W. Tsang and S. A. Zahra, "Organizational unlearning," *Human Relations*, vol. 61, no. 10, pp. 1435–1462, 2008, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1177/0018726708095710>
- [50] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1080/0144929X.2012.708787>
- [51] S. Zhuo, R. Biddle, Y. S. Koh, D. Lottridge, and G. Russello, "Sok: Human-centered phishing susceptibility," *ACM Trans. Priv. Secur.*, vol. 26, no. 3, apr 2023, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3575797>

- [52] B. A. Anderson, "The attention habit: how reward learning shapes attentional selection," *Annals of the New York Academy of Sciences*, vol. 1369, no. 1, pp. 24–39, 2016, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1111/nyas.12957>
- [53] A. Bandura, *Social Learning Theory*, ser. Prentice-Hall series in social learning theory. Prentice Hall, 1977, [Accessed: July 27, 2026]. [Online]. Available: <https://books.google.de/books?id=HFokAQAAAMAJ>
- [54] M. R. A. Salah, "The influence of rewards on employees performance," *British Journal of Economics, Management & Trade*, vol. 13, no. 4, pp. 1–25, 2016, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.9734/BJEMT/2016/25822>
- [55] S. Goel, K. Williams, J. Huang, and M. Warkentin, "Understanding the role of incentives in security behavior," *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.24251/HICSS.2020.519>
- [56] J. M. Blythe, A. Gray, and E. Collins, "Human cyber risk management by security awareness professionals: Carrots or sticks to drive behaviour change?" in *HCI for Cybersecurity, Privacy and Trust*, A. Moallem, Ed. Cham: Springer International Publishing, 2020, pp. 76–91, [Accessed: July 27, 2026]. [Online]. Available: https://doi.org/10.1007/978-3-030-50309-3_6
- [57] K. Witte and M. Allen, "A meta-analysis of fear appeals: Implications for effective public health campaigns," *Health Education & Behavior*, vol. 27, no. 5, pp. 591–615, 2000, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1177/109019810002700506>
- [58] H. Leventhal, D. Meyer, and D. Nerenz, "The common sense representation of illness danger," *Medical Psychology*, vol. 2, pp. 7–28, 1980, [Accessed: July 27, 2026]. [Online]. Available: <https://www.researchgate.net/publication/303283742>
- [59] K. Renaud, R. Searle, and M. Dupuis, "Shame in cyber security: Effective behavior modification tool or counterproductive foil?" in *Proceedings of the 2021 New Security Paradigms Workshop*, ser. NSPW '21. New York, NY, USA: Association for Computing Machinery, 2022, p. 70–87, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3498891.3498896>
- [60] R. Greenbaum, J. Bonner, T. Gray, and M. Mawritz, "Moral emotions: A review and research agenda for management scholarship," *Journal of Organizational Behavior*, vol. 41, no. 2, pp. 95–114, 2020, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1002/job.2367>
- [61] L. Schöni, V. Carles, M. Strohmeier, P. Mayer, and V. Zimmermann, "You know what? - evaluation of a personalised phishing training based on users' phishing knowledge and detection skills," in *Proceedings of the 2024 European Symposium on Usable Security*, ser. EuroUSEC '24. New York, NY, USA: Association for Computing Machinery, 2024, p. 1–14, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3688459.3688460>
- [62] K. Renaud, "Blaming noncompliance is too convenient: What really causes information breaches?" *IEEE Security Privacy*, vol. 10, no. 3, pp. 57–63, 2012, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1109/MSP.2011.157>
- [63] I. Kirlappos, S. Parkin, and M. A. Sasse, "Learning from "shadow security": Why understanding non-compliant behaviors provides the basis for effective security," *Workshop on Usable Security (USEC'14)*, 2014, [Accessed: July 27, 2026]. [Online]. Available: <https://discovery.ucl.ac.uk/id/eprint/1424472/>
- [64] —, "Shadow security" as a tool for the learning organization," *SIGCAS Comput. Soc.*, vol. 45, no. 1, p. 29–37, Feb. 2015, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/2738210.2738216>
- [65] P. Puhakainen and M. Siponen, "Improving employees' compliance through information systems security training: An action research study1," *Management Information Systems Quarterly*, vol. 34, no. 4, pp. 757–778, 12 2010, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.2307/25750704>
- [66] A. Charalambous, A. Piki, and E. Stavrou, "Redesigning cybersecurity awareness-raising and training programs: insights from professionals on knowledge, skills and educational practices," *Information and Computer Security*, vol. 34, no. 2, pp. 273–294, 08 2025, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1108/ICS-04-2025-0163>
- [67] H. de Bruijn and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, no. 1, pp. 1–7, 2017, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.giq.2017.02.007>
- [68] R. Pankus, M. Ninow, S. Fahl, and K. Marky, "Privacy mental models of electronic health records: A german case study," in *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. Anaheim, CA: USENIX Association, Aug. 2023, pp. 525–542, [Accessed: July 27, 2026]. [Online]. Available: <https://www.usenix.org/conference/soups2023/presentation/pankus>
- [69] K. Jenni and G. Loewenstein, "Explaining the identifiable victim effect," *Journal of Risk and uncertainty*, vol. 14, no. 3, pp. 235–257, 1997, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1023/A:1007740225484>
- [70] R. W. Reeder, I. Ion, and S. Consolvo, "152 simple steps to stay safe online: Security advice for non-tech-savvy users," *IEEE Security Privacy*, vol. 15, no. 5, pp. 55–64, 2017, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1109/MSP.2017.3681050>
- [71] S. Jin, H. Baek, U. Lee, and H. Kim, "I was told to install the antivirus app, but i'm not sure i need it: Understanding smartphone antivirus software adoption and user perceptions," in *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, ser. CHI '25. New York, NY, USA: Association for Computing Machinery, 2025, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1145/3706598.3713452>
- [72] A. Beautelement, R. Coles, J. Griffin, C. Ioannidis, B. Monahan, D. Pym, M. A. Sasse, and M. Wonham, *Managing Information Risk and the Economics of Security*. Springer, Boston, MA, 2009, ch. Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security, pp. 141–163, [Accessed: July 27, 2026]. [Online]. Available: https://doi.org/10.1007/978-0-387-09762-6_7
- [73] I. Kirlappos and M. A. Sasse, "Fixing security together: Leveraging trust relationships to improve security in organizations," in *USEC 2015*. Internet Society, 2015, [Accessed: July 27, 2026]. [Online]. Available: <http://dx.doi.org/10.14722/usec.2015.23013>
- [74] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the human aspects of information security questionnaire (hais-q)," *Computers Security*, vol. 42, pp. 165–176, 2014, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.cose.2013.12.003>
- [75] U. N. Danner, H. Aarts, and N. K. de Vries, "Habit vs. intention in the prediction of future behaviour: The role of frequency, context stability and mental accessibility of past behaviour," *British Journal of Social Psychology*, vol. 47, no. 2, pp. 245–265, 2008, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1348/014466607X230876>
- [76] D. T. Neal, W. Wood, J. S. Labrecque, and P. Lally, "How do habits guide behavior? perceived and actual triggers of habits in daily life," *Journal of Experimental Social Psychology*, vol. 48, no. 2, pp. 492–498, 2012, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1016/j.jesp.2011.10.011>
- [77] D. Ashenden and D. Lawrence, "Security dialogues: Building better relationships between security and business," *IEEE Security Privacy*, vol. 14, no. 3, pp. 82–87, 2016, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.1109/MSP.2016.57>
- [78] M. Frank and V. Kohn, "How to mitigate security-related stress: The role of psychological capital," *Proceedings of the 54th Hawaii International Conference on System Sciences*, 2021, [Accessed: July 27, 2026]. [Online]. Available: <https://doi.org/10.24251/HICSS.2021.550>
- [79] M. Frank, "Sharing information security failure: The role of social context and social environment," *PACIS 2020 Proceedings*, 2020, [Accessed: July 27, 2026]. [Online]. Available: <https://aisel.aisnet.org>
- [80] R. Bjork and E. Bjork, *From Learning Processes to Cognitive Processes: Essays in Honor of William K. Estes*. Erlbaum, 1992, vol. 2, ch. A new theory of disuse and an old theory of stimulus fluctuation, p. 35–67, [Accessed: July 28, 2026]. [Online]. Available: <https://www.researchgate.net/publication/281322665>
- [81] A. S. Schöffler, C. Thim, J. Haase, N. Gronau, and A. Kluge, "Information processing in work environment 4.0 and the beneficial impact of intentional forgetting on change management," *Zeitschrift für Arbeits- und Organisationspsychologie AO*, vol. 64, no. 1, p. 17–29, 2020, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1026/0932-4089/a000307>
- [82] R. S. Kuckartz, Udo and, *Qualitative Inhaltsanalyse. Methoden, Praxis, Umsetzung mit Software und künstlicher Intelligenz*. Beltz Juventa, 2024, [Accessed: July 28, 2026]. [Online]. Available: <https://beltz.de/BEL447912>
- [83] "Acm code of ethics and professional conduct," *Commun. ACM*,

- vol. 35, no. 5, p. 94–99, May 1992, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1145/129875.129885>
- [84] American Psychological Association, “Ethical Principles of Psychologists and Code of Conduct,” *American Psychologist*, vol. 57, no. 12, pp. 1060–1073, 2002, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1037/0003-066X.57.12.1060>
- [85] W. M. Association, “World medical association declaration of helsinki: Ethical principles for medical research involving human participants,” *JAMA*, vol. 333, no. 1, pp. 71–74, 01 2025, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1001/jama.2024.21972>
- [86] F. Herbert, S. Becker, L. Schaewitz, J. Hielscher, M. Kowalewski, A. Sasse, Y. Acar, and M. Dürmuth, “A world full of privacy and security (mis)conceptions? findings of a representative survey in 12 countries,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’23. New York, NY, USA: Association for Computing Machinery, 2023, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1145/3544548.3581410>
- [87] N. Eyal, *Hooked: How to Build Habit-Forming Products*. Penguin Books Limited, 2014, [Accessed: July 28, 2026]. [Online]. Available: <https://books.google.de/books?id=R42aBAAQBAJ>
- [88] P. Lally and B. Gardner, “Promoting habit formation,” *Health Psychology Review*, vol. 7, no. sup1, pp. S137–S158, 2013, [Accessed: July 28, 2026]. [Online]. Available: <https://doi.org/10.1080/17437199.2011.603640>

APPENDIX

A. Guiding Questions of the Workshops

PREPARATION: Secure & Insecure Behaviour.

- 0.1) What insecure behaviours have you recently observed in your own or another organisation, or among colleagues?
- 0.2) What would be secure alternatives?
- 0.3) As a group, decide on one secure behaviour and one matching insecure behaviour that you would like to examine further during this workshop.

STAGE 1: Feasibility of Secure Behaviour.

- 1.1) What conflicts may arise between employees’ primary tasks and the new secure behaviour?
- 1.2) How could employees circumvent the secure behaviour?

STAGE 2: Security Awareness.

- 2.1) How do you currently raise security awareness among your employees?
- 2.2) What are the (additional) benefits of the new secure behaviour?
- 2.3) How can you highlight these benefits to your employees?

STAGE 3: Information about Risks & Motivation to Change.

- 3.1) Who are potential attackers on the old insecure behaviour?
- 3.2) How would attackers exploit the old insecure behaviour, and what data and systems could be at risk?

STAGE 4: Understanding Correct & Incorrect Behaviour.

- 4.1) How does the new secure behaviour prevent attacks from occurring?
- 4.2) What **do’s** should employees follow to implement secure behaviour?
- 4.3) What **don’t’s** should employees avoid to implement secure behaviour?

STAGE 5: Agreement through Co-Design.

- 5.1) How can you enable your employees to express questions and concerns about the new secure behaviour?
- 5.2) How can employees help shape the introduction and implementation of the new secure behaviour?

STAGE 6: Self-Efficacy through Successful Trial & Error.

- 6.1) How can employees try out or observe the new secure behaviour?
- 6.2) How can you avoid that employees feel anxious or fail in the process?

STAGE 7: Implementation through Environmental Redesign.

- 7.1) Which cues could trigger the old insecure behaviour?
- 7.2) How can you redesign the work environment to eliminate these triggers?
- 7.3) How can you make the new secure behaviour the easiest option?

STAGE 8: Embedding in Everyday Work.

- 8.1) How can you encourage your employees to adopt the secure behaviour?
- 8.2) How can you reward the adoption of the secure behaviour?

STAGE 9: Secure Behaviour is Habit

- 9.1) How can you continuously reward the secure behaviour?
- 9.2) What counts as deliberate refusal/circumvention of the secure behaviour?
- 9.3) How can deliberate refusal to behave securely be sanctioned?