"Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting

Jonas Hielscher
Human Centred Security, Ruhr University
Bochum, Germany
jonas.hielscher@ruhr-uni-bochum.de

Annette Kluge
Work and Organizational Psychology, Ruhr University
Bochum, Germany
annette.kluge@ruhr-uni-bochum.de

Uta Menges
Work and Organizational Psychology, Ruhr University
Bochum, Germany
uta.menges@ruhr-uni-bochum.de

M. Angela Sasse
Human Centred Security, Ruhr University
Bochum, Germany
angela.sasse@ruhr-uni-bochum.de

Abstract

Security awareness is big business – virtually every organization in the Western world provides some form of awareness or training, mostly bought from external vendors. However, studies and industry reports show that these programs have little to no effect in terms of changing the security behavior of employees. We explain the conditions that enable behavior change, and identify one significant blocker in the implementation phase: not disabling existing (insecure) routines – failure *to take out the trash* – prevents embedding of new (secure) routines. Organizational Psychology offers the paradigm Intentional Forgetting (IF) and associated tools for replacing old (insecure) behaviors with new (secure) ones by identifying and eliminating different cues (sensoric, routine-based, time and space based as well as situational strength cues) that trigger old behavior. We introduce the underlying theory, examples of successful application in safety contexts, and show how its application leads to effective behavior change by reducing the information that needs to be transmitted to employees, and suppressing obsolete routines.

CCS Concepts

• **Security and privacy** → *Social aspects of security and privacy.*

Keywords

Human Factors, Intentional Forgetting, Unlearning, Security Awareness, Socio-technical systems, Information Overload

ACM Reference Format:
Jonas Hielscher, Annette Kluge, Uta Menges, and M. Angela Sasse. 2021. "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. In *New Security Paradigms Workshop (NSPW '21), October 25–28, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3498891.3498902

NSPW '21, October 25–28, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8573-2/21/10.
https://doi.org/10.1145/3498891.3498902

1 Introduction

Security awareness is big business, already amounting to $1 billion in 2017 and is estimated to grow up to $10 billion[1] by 2027. The market is perceived as far from saturated – even security vendors whose core business is technical products and services are increasingly heading into that market.

Are organizations getting their money's worth in return? It depends what they are trying to achieve – if their aim to comply with standards or regulations that demand *mandatory security training*[2] and that auditors can *tick the box* if material exists, or the organization can show that a certain percentage of employees has completed it, that may be sufficient. For organizations that actually rely on specific secure behaviors by their employees to manage risks, literature that shows that these efforts do not change security behaviors should raise concerns. An industry survey of over 100 major companies [49] concluded that traditional training offerings – which raise awareness of threats and risks, and do's and don'ts employees should follow – has little effect in terms of changing behavior of employees – it concludes they are *just background noise.* Employees are largely aware of what they should and should not do, but often don't follow those behaviors in practice. Bada et al. [9] reviewed national security awareness campaigns, and came to the same conclusion.

Several papers over the past decades and reports have highlighted one major reason: that most organizations don't carry out a *feasibility check* of the secure behaviors they proscribe. It has been shown that some mandated security behaviors are impossible for employees to carry out, and others would reduce employees' productivity to such a degree that they feel compelled to *cut corners* [12]. The UK NCSC has coined the term security *rule-bending* for this type of non-malicious non-compliant behavior [71]. Many organizations are tacitly complicit and turn a blind eye to the fact that employees don't follow mandated rules, rather than investigating the cause of non-compliance and finding ways to secure the organization in a way that preserves productivity, as recommended by Kirlappos et al. [53] and the NCSC. But not ensuring feasibility

[1] https://cybersecurityventures.com/security-awareness-training-report/, accessed May 04th 2021
[2] In the U.S. e.g. required by the Federal Information Security Management Act or the Health Insurance Portability and Accountability Act, https://symbolsecurity.com/2020/09/10/regulatory-compliance-and-security-awareness-training/, accessed May 11th 2021

reduces or negates the effectiveness of the security measures the organization has put in place. Seeing security rules not being followed also creates the impression among employees that not following them is ok – a corrosive effect that led General Douglas MacArthur to coin the maxim "Never give an order that can't be obeyed" [93]. In summary – organizations that want effective protection should make sure their rules can actually be followed. Usable security researchers have pointed out over that past two decades that security is a secondary task for everyone except security experts [14, 27, 81], meaning that secure behavior has to be possible within the context of the primary task that employees are focused on, i.e. within the time constraints, focus of attention and cognitive load the primary task requires [37].

The good news is that security behavior that are feasible and carried out frequently become automatic – routines that employees can perform without thinking. Daniel Kahnemann famously coined the term *fast thinking* to describe this mode, distinguishing it from the deliberate, step-by step *slow thinking* mode in which we tackle tasks that are new or which we encounter infrequently [51]. The distinction between automatic and deliberate behavior is well-established in human factors [72, 73] and has been applied to IT security in a previous NSPW paper [19]. Human productivity is largely based on our ability to turn frequent behavior into routines or habits – *fast behavior*. The downside is that a well-established habit or routine, once embedded, is hard to remove. The English schoolmaster Ivor Benyon expressed his exasperation at the difficulty to get rid of 'bad habits' in the following ditty:

"*The trouble with habits is that they are hard to get rid of.*
If you get rid of the 'h' you still have abit.
If you get rid of the 'a' you still have a bit.
If you get rid of the 'b' you still have it."

And in their bestselling book *Switch*, Chip & Dan Heath pointed out that replacing an existing habit or routine is actually not at all like flicking a switch, but more like turning around an elephant [43]. The terms 'habit' and 'routine' denote the same concept, but in this paper we will use the term routine throughout.

Routines which have been executed and applied for years are stored in memory with a high storage strength [17, 18]. Established through a high number of repetitions, routines are easy to access and fluently executed when required in a specific situation and are executed without conscious control. Particular cues in the environment (e.g. the OK button of a pop-up message) trigger the instantaneous recall of a routine with high storage strength (click to OK to proceed), and immediate execution. This is one reason for being "fast". Even when such routines have not been recalled and executed for a while (which can be years) routines with high storage strength can "break through", press forward and make their way to being recalled and executed without conscious control, e.g. in the face of time pressure or other forms of perceived stress.

A second reason for being fast is the high retrieval strength of a routine that has been carried out for years. Routines that are carried out on a daily basis also possess a high retrieval strength: They are very easy to recall and access from memory. But the combination of high storage strength and high retrieval strength of routines also makes us vulnerable to attacks which trigger routines in inappropriate contexts – for instance when we receive an email that asks us to confirm our username and password on a site that at first glance looks legitimate. Security experts advise users to *take 5* (presumably minutes), or *stop and think*, i.e. abandon the routine behavior and switch to the *slow* model. This advice is neither realistic – the productivity reduction that would result from conducting our lives in the "slow" lane in the name of security would be unaffordable – nor does it guarantee security. Humans make errors in slow as well as fast mode – just different ones. Social engineering attackers, for instance, often put their targets in *slow* mode, flood them with information to divert attention, and then activate the routine that gives them what they want (e.g. the password). Or, they create a stressful situation, knowing that people in such situations resort to embedded routines ("One of the goals of manipulation can be to create anxiety stress" [41]).

This means it is really very much in the organization's best interest to ensure their employees adopt secure routine behaviors, while being aware of the contextual limitations that apply to them.

The 2015 RISCS White Paper *Awareness is Only the First Step* highlighted that knowledge about risks and correct behavior is not enough to embed those behaviors [15]. Yet, most organizations currently do nothing or little to support their staff through those additional steps. Current security awareness materials proscribe secure behavior and expect compliance (adherence), rather than establishing concordance to get employees on board [7], they do not provide opportunities to rehearse new behaviors and build confidence (self-efficacy) – all of which we examine in more detail in section 2.1. But even when some measures to support behavior change are added – in particular, *nudges* have been popular in recent years [24] – behavior often does not change for good. The main reason is that employees keep encountering familiar cues that trigger old existing (insecure) routines, and re-inforce those instead of the new secure behaviors. To enable successful behavior change, organizations need to remove these cues and disable old routines – i.e. *take out the trash*.

Intentional Forgetting (IF) is an organizational design approach that has been successfully applied to transform safety behavior, and in this paper we outline how it can be applied to transform security behavior. IF in the organization aims at deliberately reducing the retrieval strength of unwanted routines by reducing the trigger cues that would recall them. In security, the need to *take out the trash* – removing cues, decommissioning obsolete terms, and adapting user interfaces to reflect a change in policies – in order to reduce the recall of unwanted insecure routines is currently not well understood, and IF provides the framework for changing this. To illustrate how IF would be applied, consider the topical issue of securely working from home during the COVID pandemic. Remote work brings new challenges to IT security and consultancy companies, VPN providers and federal agencies created new products, rules and training [20]. Employees are told to behave differently, e.g. that they should log into the VPN first, that they should not let relatives or friends into their home office while working material is accessible to others (even though their 'home office' may be in a shared space, such as kitchen or living room), that they should secure their private WiFi, should not mix up private and professional IT. But at the same time, the cues that drive their behavior with high retrieval and storage strength remain the same. We may now work from a laptop at home, but we still interact with the

same internal colleagues and external customers via the same email applications and messages, and we authenticate the same way. Exhortations to be extra vigilant, check that messages are genuine and have not been tampered with, will be quickly forgotten once employees are 'in the flow' of work routines. More information does not help when cues trigger unwanted routines (leading to *fast thinking*) that might be insecure in the home office. Employees need support to 'unlearn' obsolete routines: old cues must be eliminated and replaced with other cues that trigger new routines. This paper explains how employees can 'unlearn' through design and support measures provided by organizations.

The remainder of this paper is structured as follows. In section 2, we explain why raising security awareness does alone not increase the security within organizations. We also introduce the basic concepts of IF drawn from the organizational psychology literature. In section 3, we briefly look at the problem that comes with too much and conflicting security advice. In section 4, we take a closer look at three well studied examples of newly introduced security measures that are not used by employees due to the parallel availability of old measures and routines. In section 5, we draw first ideas on how IF could be applied in the field of IT security. In section 6, we discuss our paradigm and explain how further research and intervention could look like. In section 7 we conclude our ideas.

2 Background

In this section we first explain the steps that need to be completed until the a new behavior is embedded. We explain where IF fits into the other activities organizations need to engage in to support employees transitioning through those steps, and then examine the theory of IF, the state of the research in this field, and how it can be applied.

2.1 Why Security Awareness (alone) is not Effective

In 2015, a RISCS White Paper pointed out that current security and training approaches only push information [15]. They expect that – once employees have understood the risks and know what to do to avoid them – they will change behavior. But information alone rarely leads to behavior change. This has always been true, but is even more so today:

> *"We live in the single-most information-overloaded, stimulation-saturated environment that has ever existed. People just don't have the capacity to fully consider every piece of information in their time-scarce, attention-challenged, busy lives."* [59]

Providing information to employees will not enable them to replace existing (what Kahnemann termed *fast*) insecure routine behaviors with secure ones. For a new behavior to *stick*, it has to be repeated over a period of roughly 28 days to become routine, and the following five factors are required to support employees through that phase (see also figure 1):

(1) **Security Hygiene**: The necessary condition for any behavior change it that target behavior is actually possible. This may sound rather obvious, but research over the past two decades has identified proscribed security behaviors are in practice impossible, or consume so much productivity that employees bypass them to protect their job performance (e.g. finding the security features in Microsoft Word [36], or following policies for strong password [82], or distinguishing between simulated and real phishing emails and genuine communications [95]). Organizations should not mandate security behaviors without carrying out a feasibility check first, and if necessary "restructure practices and policies, to better align with people's workplace goals and/or capabilities" [29].
(2) **Establish concordance**: IT security has traditionally cast employees in a passive role – the company mandates policy, employees *comply or die* – a behavior known as adherence. Adherence does not require consent, but constant monitoring, enforcement and sanctions – something that can work when the organization has plentiful resources, e.g. in the military. In other areas its success has been *hit-and-miss* at best even in medicine – where behavior change benefits the person not an organization – from patients taking their medication to smoking cessation and weight loss [62]. Behavior change is more likely when people have a chance to commit to the goals, and agree on the steps required to reach those goals are feasible. The approach of building concordance rather than demanding adherence has been applied in security by Ashenden & Lawrence [7].
(3) **Enabling self-efficacy**: As well as agreeing that they want to change behavior, employees need to have confidence in their own ability to succeed. Most people won't embark on a new behavior if they think they will not succeed and fail. Many organizations with physical access control systems still have problems with tailgating, and are puzzled why employees don't follow the instruction that they should challenge someone who tries to sneak through the gate behind them. Beautement et al. [11] report that employees were aware they were supposed to challenge tailgaters, but did not do so because they were not confident about managing the situation, which might lead to an unpleasant confrontation. Organizations can help employees build self-efficacy through direct experience (e.g. being shown how to challenge someone in a non-confrontational manner, and trying it in role-playing exercises) or vicarious experience (watching a video of someone you can empathize acquire the new behavior and perform it successfully).
(4) **Implementation**: once concordance and self-efficacy have been built, employees have to be reminded to stop the unconscious execution of "old" routines with high storage and retrieval strength, and consciously choose the new secure behavior. While the new behavior is bedding in (aka is becoming proceduralized), employees need to be reminded that and why they are choosing the new secure behavior.
(5) **Embedding**: The new secure behavior has to be repeated many times to become embedded and proceduralized to acquire a high storage strength for its own. New behavioral patterns need to be accumulated with high storage and retrieval strength in order to win the competition against the unwanted fast behavior that tries to break through when a particular cue is available. With every repetition of the new behavior, we move forward on the path to automaticity and high storage strength, but every time the unwanted insecure

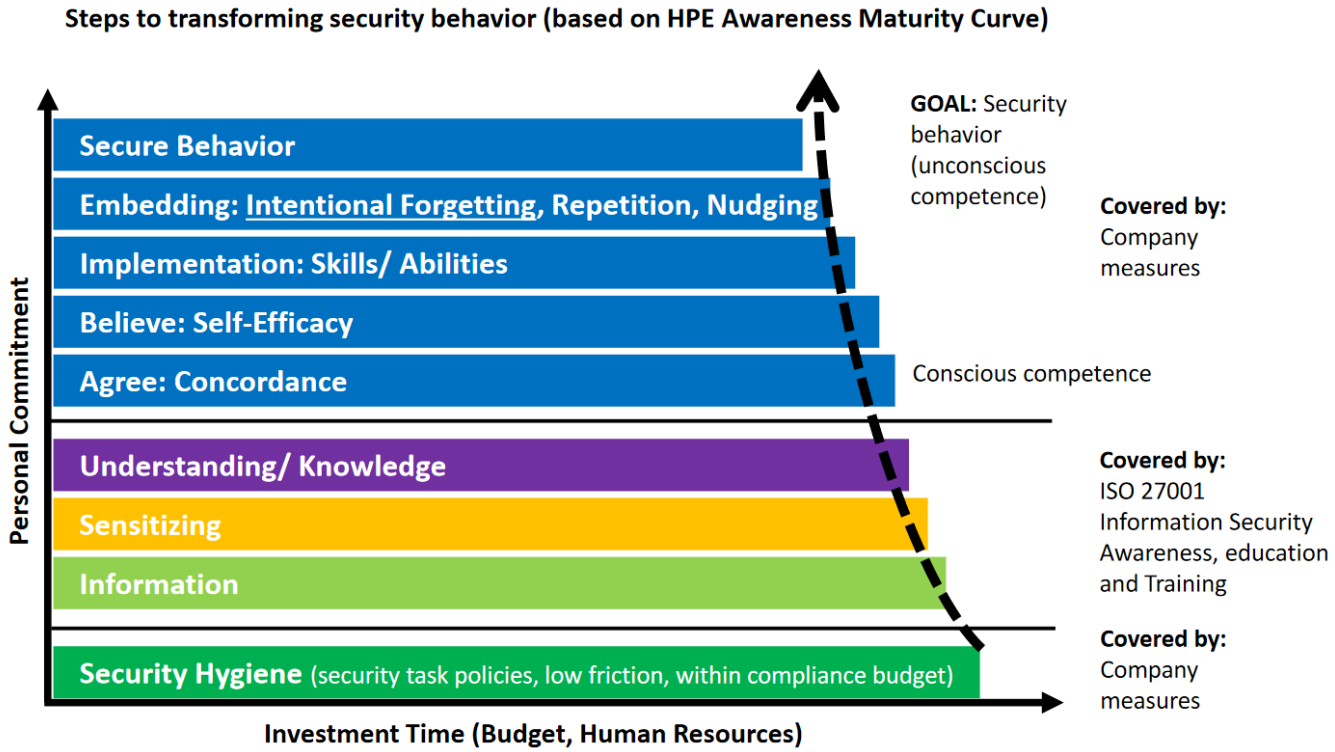

Figure 1: Steps to adopting new security behavior (new version of figure originally presented in [15]).

behavior is carried out, we go several steps back in terms of storage and retrieval strength while giving the unwanted routine the opportunity to become even stronger. Companies need to take active steps to decommission old behaviors, and remove the cues or triggers for them and support IF.

This last step is a crucial one, and where embedding of the new security behavior often fails. This has been recognized in the world of workplace safety, and in the past five years a design approach called Intentional Forgetting (IF) has been applied to prevent this *failure on the last few yards*, and help new behaviors to become embedded. The parallels between safety and security behaviors in the organizational contexts have been highlighted before: Brostoff & Sasse [19] for instance applied the Human Error framework [72] to show that human *failure* to follow the password policies to regularly replace old passwords were predictable because they ignored the workings of long-term memory. Since then, knowledge about the limitations of short-term memory have led to the design of workable one-time authentication [74], and understanding of how long-term memory works has reduced the reliance on strong passwords, and password expiry being largely abolished. Another aspect of human memory is that routine behaviors are strongly embedded. Attempts to replace an existing routine behavior with a new secure behavior fails if the old continues to be reinforced by not de-commissioned old behaviors properly, and leaving triggers in place – if you will, failure to *take out the trash*. Once organizations are aware of this, they can apply a systematic approach to remove cues that lead to old and insecure behavior and smooth the path to adopting new secure ones.

2.2 Intentional Forgetting

IF is considered as a goal-directed process in response to an explicit or implicit cue to forget [28]. The aim of IF is to reduce the influence of old routines [39] and to stop old knowledge from being used [46]. IF is understood as the motivated attempt to limit the future recall of a defined memory element that is no longer needed for execution – and interferes with the embedding of the new behaviors. These processes of IF are required for the adaptation to new organizational conditions and mechanisms such as unlearning, discarding and replacing routines – such as removing insecure behaviors and establishing new secure ones – rearranging, ignoring, and deleting [28, 55].

Forgetting is essential to the facilitation of change, especially when current knowledge is perceived as an obstruction and a competitor to new knowledge [60]. Unlearning as one facet of forgetting, in the sense of discarding and replacing old routines, is assumed to support the objective to install new routines. Kluge & Gronau [54], proposed that forgetting is an important process, as a high amount of available and stored knowledge can also lead to difficulties in interpreting information and might impede the evaluation of alternative ways to reach organizational goals. IF is particularly relevant in the organizational context of implementing routines that differ from the routines that have been performed and executed with high levels of proceduralizations. It is a deliberately chosen process

to impede the recall of certain routine [88], procedures or *way of doing things*, and to not provide cues for triggering "old routine" in the case of a certain query in order to support an organization's changed strategic goal achievement [67]. This central role that forgetting plays in the quest to transform insecure behaviors to secure ones has so far been overlooked.

To deliberately initiate the forgetting of certain routines, organizational routines need to be suppressed. Organizational routines are "multi-actor, interlocking, reciprocally-triggered sequences of actions" [22]. Routines are the relevant source of stability, reliability and speed of organizational transformation processes [13]. Organizational routines differ with respect to their content, structure, sequence in time, amount of formalization and the required knowledge (in terms of memory items) that needs to be applied.

The starting point to IF in organizations is eliminating cues that otherwise would trigger the recall of unwanted behaviors. If a particular cue is missing over a longer period of time, resulting in no recall of the old routine, the retrieval strength of the memory item associated with the retrieval cue is reduced and forgetting commences [18]. In this regard, it is important to mention that various cues differ in salience. This assumption is supported by event system theory (EST), according to which new, critical or disruptive events become salient [63]. Retrieval cues that are no longer presented cannot trigger unwanted routines, and new secure behaviors are given the opportunity to be performed instead. Four cue types are considered as important in the forgetting of organizational routines [54]:

(1) **Sensory cues**, which are the basal cues such as smell, taste, light, color, sound, tactile perceptions, temperature, or physical pain that trigger the recall of certain memory items (visual, olfactory, oral, tactile). For most employees this can be that the Desktop environment, the applications they use and the content of their desks look always the same. If a new fancy security tool is introduced (a password manager, an encrypted messenger, a VPN or anything else) the visual environment won't have changed. While the environments have changed in the home office the Desktop and Applications havn't. In order to implement new rules, like the usage of the VPN, those cues that remind the employees of the old routines need to be changed or removed in order for the new security behaviors to have a chance to bed in.
(2) **Routine-related cues**, which include actor-related, object-related, sequence of task-related and information-related cues (see figure 2). If the virtual team meeting takes place at the same time and the same way as in the office, this 'business as usual' reinforces existing routines. Routines can be changed in different ways: Either by removing one element in the routine-change, by replacing it, or by changing the order. Multiple scenarios with such changes are thinkable, in the routine of the daily work but also in the routine of an application flow.
(3) **Time and space cues**, which include stimuli indicating location (e.g., production site) and time (of year, week, day) of the execution of the routine. For example, can the entrance to a building or an office be related with the routine to open doors for others (which allows tailgating), the start of the working day with the quick check of all emails (which might allow phishing) and the desk in the office with the routine to write down passwords on notes.
(4) **Situational Strength Cues**, which include implicit or explicit cues provided by external entities (e.g., supervisors) regarding the desirability of potential behaviors. Situational strength results in a psychological pressure on the individual to show or not show particular behaviors. Security advice is usually delivered by security experts, via email or web pages. However, it is important that those giving advice are approachable and not far away, behind an email.

Identifying the cues that trigger the recall of unwanted behavioral patterns, and removing them, is a necessary part of change management interventions. Without it, all other organizational efforts spent on communicating a vision, training and enabling workers to behave according to the vision, as well as reinforcing and institutionalizing new routines will be wasted. Successful change requires removing all cues that might recall old routines. Only addressing the new routines while cues recalling old routines are still present leads to a lack of clarity, inconsistency and mixed messages [54].

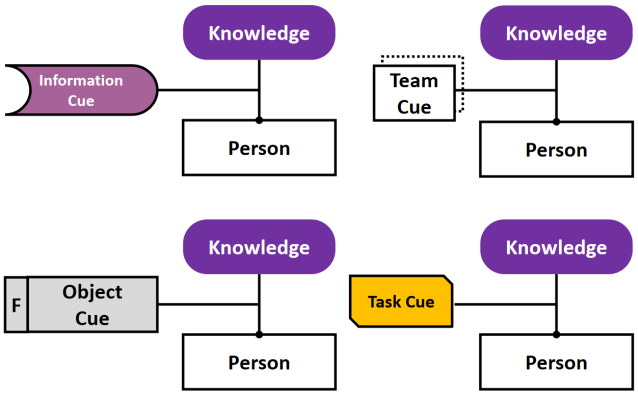

Figure 2: Routine-related cues can have different sources: 1) Information, 2) Teams, 3) Objects, 4) Tasks. Figure based KMDL Modeling language from [58], page 29.

Empirical studies on an individual level show that not all elements of a routine are forgotten at the same speed. Particular elements of a multi-actor routine (routines that include multiple employees) are even more difficult to transform - until every team member stops using the old routine, they will keep triggering and reinforcing them in each other [54, 85]. Forgetting of elements of a routine also depends on the required change (e.g. to not execute a certain element in a routine, or to execute it slightly differently, or to add an action to a well learned action). Based on those results, looking at required changes in elements of a routine can help to better predict what the difficult parts and stumbling blocks of forgetting are.

Perceived time pressure also impedes forgetting and increases errors [40, 72]: outdated behavior is more often performed unchanged when employees are under time pressure. When facing competing demands – such as being under time pressure and trying to learn a

new behavior – employees tend to 'fall back' on old routines. Based on the data analyzed so far, it was additionally found that also person related variables play an important role. Retentively as a facet of intelligence as well as subjectively perceived switching costs (in terms of effort needed) proved to be important predictors for the speed of forgetting of old routines [40]. Retentively supports forgetting (for people with high retentively it is easier to learn the new requirements of a routine while simultaneously overwriting the old one), while subjectively perceived high switching cost impedes forgetting.

3 Information- & Compliance-Overload

Many employees today feel overloaded with expectations about how they should behave to secure corporate IT and data [12, 35]. The bigger an organization grows, the larger the risk that different departments have their own very specific requirements for employees: CISOs might try to implement the latest fancy tooling, without consolidating those who need to adapt to it [8]. The legal and compliance departments might want to stick to ISO 27001 and are regularly sending internal audit teams. Team leaders are worried that their Key-Performance-Indicator (KPI) will drop when a security incident happens, and are pushing their teams with fear appeals. The data privacy manager wants to stop the spreading of data between departments. The IT-departments have their own structures, need to handle the everyday business. And this might only be the beginning of a long list. In case all of those IT security key-players are working on their own, employees are overwhelmed with information in the form of more advice and rules via email, awareness campaigns, training and the regular introduction of new tools. And even in case the departments work together, to the best of our knowledge, there are no efforts in either research or practice to remove outdated knowledge and routines. But with every update to a rule or a tooling, previous routines become obsolete and might lead to reduced productivity or security problems.

There is empirical evidence that even IT security experts don't agree about the most basic and important IT security advice – Reeder et al. [70] got 152 answers from 200 experts when asking for *3 most important* bits of security advice. The lack of coherence and diversity of language increases the 'comprehension work' required to work out which rules to follow, when, and as a result, the intended recipients just switch off [23]. Beautement et al. [12] found that there is a limit to the amount of productive time employees will sacrifice for security; but when incidents occur, organizations tend to introduce more rules [26] instead of ensuring that the rules can be followed without sacrificing productivity.

The research into usable security solutions is fortunately growing, starting with the question why users didn't use email encryption back in 1999 [97]. While single security tools might be designed in ways that users are easily able to use them and such is verified in lab experiments and with surveys and interviews, the research on how well these tools fit into the organizational context and into the every-day-routine of employees is limited. With the introduction of new tools, there is a risk that employees will develop a routine of bypassing them, for example when new security warnings occur [3, 5]. The tools also often just stack up on existing tooling and employees don't see how the new tools support their every day routine. Even if they might be trained on new tools and be initially positively minded about it, the long term memory won't change its structures as long as all the old cues are still in place. Also, the adoption of new tools is heavily supported in case teams or even complete organizations shift to the new tools at the same time.

Research following attempts to improve the secure development of software products found that having security consultants help developers only had a short-time effect – the behaviors they had been taught did not become a routine [4]. While the authors identified some additional factors that impeded change (such as that the organizational culture was partly in conflict with the desire of the developers), the software development process remained the same and kept triggering the insecure routines, instead of the new secure ones they had been shown. For example, if a security issue was written down in a common defect ticket and such a ticket was the beginning of a well established (old) development routine. All other factors associated with the old routine also stayed in place: The same colleagues, the same development software, the same managers. Hence, it seems like it was not possible for the development team to forget about the old behavior.

Another example that shows information overload and rules in conflict with each other are password policies. Password policies and advice changed and still change regularly. Despite multiple efforts to overcome passwords at all, they are still used and are the most important authentication mechanisms [45]. "Use a strong password", "Use at least 13 characters", "Combine real words", "Replace characters with digits", "Never use something you can find in a dictionary", "Use a password manager", "Don't use notes on your Desktop", "Write down your master password. You can never lose it or your data is lost", "Use a strong master password you can easily remember", "Never use a password twice", "Don't give your passwords to others", "Use a password-generator", "Change your password regularly" [42], "Change your password only after a data-breach", "Check your passwords for breaches", are examples of different, partly obsolete and contradicting advice given to users. The amount of advice, the changes in compliance rules over the years and the differences between password-enforcements on different websites [38] make it hard to securely choose and handle passwords [57]. Often the rules are even different in one organization, in case legacy applications are not updated to newer rule sets. This overwhelming number of advice can lead to the non-acceptance of rules and even to shadow security [53], where own rules and best-of's are implemented.

Our final example is the question of how employees should behave when they observe tailgating. Depending on their own social background and experiences a number of reactions are possible, from passive ignoring, active confrontation of the tailgater to the consultation of security personnel [21]. Even if the company policy states exactly what to do, employees might be used to previous behavior in addition to social pressure. In that respect, IF can provide helpful interventions in order to reduce overload by looking for obsolete, redundant and conflicting rules and by "taking out the trash".

4 Exemplary Problems

A variety of examples of failed implementations of IT security measures can be found in the literature. More specifically, interviews and surveys with employees and users often reveal that the adoption rates of new security measures are limited. In the following we examine such problems and show how IF can help to overcome them.

4.1 Password Manager

Password managers are an example of a secure way of relieving the password problems described in the previous section. Whilst one early study Steves et al. [89] found employees keen to adopt it even when the non-usage was not sanctioned by their organization – but mostly to reduce the number of times they had to enter the passwords. Those who struggled to recall passwords used a different coping strategy: re-using the same passwords to increase storage and retrieval strength, or writing them down. Once such a coping strategy has become a routine, people are reluctant to change it. Pearman et al. [66] interviewed 30 participants and found that of nine who did not use any password management tool, six didn't because they were satisfied with their current approach (writing down). Fagan et al. [32] reported that 50% of the 38 participants of a survey didn't use password managers because they trusted in their current password remembering mechanism. Alkaldi et al. [1] also reported many of their 352 survey participants state "I am already secure". Stobert et al. [90], discovered that password managers do not integrate well with the current routines of users, and tried to design an image-based manager that would integrate better into users routines. The problem that users just stick to old password management routines was confirmed by Alkaldi et al. [2] in 2021, when they performed a week long study with 198 smartphone users. Farke et al. [33] reported a similar problem with FIDO tokens: Users didn't adopt these secure tokens if they still had to the chance to use old-style passwords: that established routine offers the shortest path to their primary goal, and is reinforced every time users decide not to make the switch. Overall, setting aside time to switch to the new behavior would not be much effort, in return for much improved security – but it requires a conscious effort and planning, and resisting the shortest path to the goal.

IF can help here. The key lies in eliminating those cues that trigger old routines in order to make the routine not retrievable from memory. The most first routine-related cue that triggers the "old" password routine is to ask for a password when a user needs to set up credentials. Employees faced with impossible memory demands have developed coping strategies [89], including a password-generating routine they think they can remember and enter on the devices they use. These routines have a high storage and retrieval strength, so the cue *password* triggers a mental routine of creating a new password, based on a personal "algorithm" (In most cases, this involves stringing together a few words and embedding some numbers and special characters, to meet the password policies they have been familiar with, often enforced by checkers or strength meters.). In the worst case – from a security point of view, but extremely likely when under stress and time pressure – they will retrieve an existing password with high retrieval strength and re-use it [10]. Users might also take the service they are creating the password for into account [96], e.g. taking the name of the service as part of the password. That means that the association of users with the service they need to register for is part of the password creation routine.

The simple trigger-mechanism *password field → think up a "new" password* is further supported by other cues: many have a non-digital notebook, or a file on their desktop where they store passwords, or use a messenger to secretly send the passwords to themselves. The notebook or application Desktop icon are cues that trigger further existing coping routines users have developed for passwords. The UI of a PC looks the same wherever you use it. On smartphones, the visuals can be different every time you use an app. However, in both cases, the installation of a password manager does not change the look and feel of what users see on the devices: The applications that require the passwords stays the same, as does the operating system and desktop background – so there are no cues to trigger the use of the password manager.

Another routine that is overlooked is that users look down at the keyboard and their hands when they are creating new passwords [86]. At that point, multiple sensory-cues occur that can trigger old routines (such as the look and feel of the specific keyboard, or the objects around the keyboard). Such cues are always there, but it is only at the point of creating a password that it is a problem – users have only one focus of visual attention, and directing it away from the hands and keyboard at this point could eliminate those cues. A technical solution that supports the suppression of these routines are password managers which automatically create passwords and fill the required fields so that no user interaction is necessary. An example is Apple's Keychain.[3] This mechanism is supposed to support the suppression stronger than password managers that just suggest the automatic creation, like Firefox's password manager[4], or the 1Password browser plugin.[5] However, some users want to stay in control of their passwords [1, 69] because of fear due to unforeseen technical problems, like the unavailability of the password managers when they are needed. This is especially true when it comes to auto-generated passwords that nobody can possibly remember. This fear is of course not without reason and organizations need to actively address it, e.g. by promoting easy-to-use recovery strategies, like a 24/7 support desk able to restore access with new passwords immediately. Past experiences with unreliable security tools explains why employees rely on their own passwords (with high storage and retrieval strength) as they feel they are in control (of their memories). That confidence – self-efficacy, see section 2 is quite important and must work along with any automation of IT security routines [78].

When looking at the other most important task of password managers, the retrieval of passwords, cues are in place as well. Seitz [86], compared the mental model of classical password storage with password managers. He stated that it typically takes nine steps to login with password & username from a classical storage (like a

[3] https://support.apple.com/guide/iphone/automatically-fill-in-strong-passwords-iphf9219d8c9/ios, accessed May 11th 2021

[4] https://www.mozilla.org/en-US/firefox/features/password-manager/, accessed June 04th 2021

[5] https://addons.mozilla.org/en/firefox/addon/1password-x-password-manager/, accessed June 04th 2021

simple file), compared to only three steps with a password manager. Basically, the old routine requires a more extensive interaction with the file storage and a hopping between the applications. Multiple cues can be involved, e.g. a copy-paste-routine, the associations with the own user-name and the association with the other account names that surround the row containing the required password. Based on the routines and cues we just identified we make suggestions of IF interventions on different levels in section 5.

4.2 Public WiFi & VPN

With the wider usage of transport encryption on more and more websites, the usage of open (insecure) public WiFi becomes a smaller security risk. However, sensitive unencrypted data can still be found [64] and the meta-data of the connections, e.g. the DNS queries, can lead to privacy leaks. Despite the warnings that are known for years, users are still using public wifi, and such networks are growing, e.g. in metropolitan areas and in public transportation. A very effective measure to protect users against most privacy leaks is the usage of Virtual Private Networks (VPN). The number of organizations that offer such service for their employees and the overall usage is growing, especially during the COVID pandemic of 2020 [68]. In one report the connection over unsecure networks was even identified as a major security risk for remote workers [65]. However, for most users the usage is not in their daily routine [87], especially when they work remotely from home.

The usage of a VPN remains an optional security feature, even in the organizational context. While some applications might only be accessible when the device is connected to the internal networks via the VPN, multiple applications like Browser and Video Conferencing tools can be used without such a connection. Hence, employee should be encouraged to enable their VPN connection in addition to the technical restriction that some application might only work with VPN. IF interventions would target to break the routine of directly using online applications after the login on a device and create a new routine of activating the VPN after login. The great challenge here is that VPNs are not used inside a controllable office environment but rather from home and from different mobile workplaces. Hence, an intervention cannot change sensory cues of the environment or the daily routine. It can only work by changing cues on the device itself.

There are numerous ways to implement IF in this context: Employees could be shown a welcome text as soon as they have started their computer, which indicates that they have to connect to the corresponding VPN first. This hint can be combined with an auditory cue - a short tune. In the course of this, the classic conditioning could be used and gradually the lyrics could be omitted and only the short tune could be heard when connecting to the VPN. Alternatively, cups with inscription "Please connect to VPN" could be handed out to all employees or sent home in the case of home office. The employees could also get small desk calendars (sent home), provided with a friendly saying for each day and at the top is the note "Start VPN Client". A combination of online and offline cues could also be helpful, e.g. by sending an Outlook invitation with the daily reminder to the VPN client in addition to the paper calendar. Furthermore, ideas based on gamification could be implemented. For all these proposals, the costs incurred by companies would be kept comparatively low.

4.3 Encrypted USB Flash Drives

An older example that has been investigated in an empirical context inside an organization was the introduction of encrypted USB flash drives, as an alternative for normal unencrypted flash drives that were widely used and lost, and thus posed an unacceptable risk to many organizations [12]. Organizations demanded the switch and indeed blocked ways of downloading sensitive information to unencrypted drives, but did not support measures to support employees in making the switch. Many employees were unsure how to use the new encrypted drives correctly, and had concerns about the reliability of the new drives, so workarounds such as emailing files to external addresses became common [53]. A how-to-use-guide and an explanation of the security advantages of the new technology would have been necessary. The fact that the new flash drives looked no different from the old ones, and the same action of inserting them to download data, triggered the old routine. Compared to routines that are completely performed on the desktop, the usage of USB flash drives requires additional steps (e.g. the flash drive must be taken out of the pocket and plugged into a first device and later into another). Therefore, it can be expected that more types of cues are associated with this routine: Sensory cues occur when the hand enters the pocket, touches the flash drive, and puts it into the device. Specific space cues appear as well since an USB stick is used to transfer data to different devices, e.g. the computer of a colleague, a computer used during a presentation, or a printer.

That leaves multiple opportunities to implement IF techniques. On an individual level, the sensory cues can be changed by creating a positive association between encryption and the flash drive itself that could have a different shape and haptic. Initially, downloading could have been restricted to locations where support staff were present to explain and assist employees in downloading encrypted files, and how to open them via their own laptops. Being able to rehearse the new routine of downloading and opening encrypted files would have build self-efficacy and confidence. In the office environment, new routines need to be established on a team level. On an organizational level it would be necessary to eradicate the knowledge-base of the old routines (e.g. by deleting obsolete manuals from the organization's wikis).

5 Implementation and Adaptation of IF Principles in IT Security

Based on the routines and cues identified with the usage of old password storage and creation methods, we show how IF-led interventions can facilitate the adoption of secure behaviors. Even though we have yet to evaluate their efficacy, they are based on applications of IF in the context of workplace safety, plus relevant findings from the IT security literature that do not explicitly refer to IF, but recommends interventions consistent with it [30, 83] on three levels: (1) organization level (2) team (or group) level and (3) individual level.

IF management requires to first identify the contributing factors to insecure behavior on organizational, supervisor, and precursors of behavior level. Then the cues that with a high situational strength

trigger *old* security behaviors need to be identified, bypassed and removed. In the following sections we will discuss how such IF management can work on all three levels. There are 16 different elements that can be used to make IF [54] work. Based on those approaches, we introduce a new clustering of IF methods with the purpose of design and describe IF interventions that can practically be applied in organizations:

(1) Extent of participation: Who decides **what** should be forgotten (management, team or individual)?
(2) Type of Forgetting Process: Who decides **how** it should be forgotten?
(3) Type of Forgetting: Should something be forgotten that won't be replaced by something new (**removing**)? Or should something be forgotten that will be replaced by something new (**replacing**)?
(4) Frequency of the Intervention. Is the intervention **continuous** (e.g. an forgetting agent-team constantly observes what routines should be removed, or replaced and implements necessary measures)? Or is the intervention **episodic** (e.g. individuals are specifically told once how and what to forget)?

Some of our ideas for interventions are: **'Spotless mind squad'**: A **forgetting agent-team** (which we have christenened *'spotless mind squad'*, based the movie *Eternal Sunshine of the Spotless Mind*, where unwanted memories can be removed without trace) that constantly monitors and checks all IT security regulations & rules in practice in order to suggest the ones that can be eliminated – or at least faded out, because they can be replaced by more efficient ones. Before a new regulation is introduced, the spotless mind squad also analyses possible unintended consequences on cognitive workload, effort, productivity and for organizational climate – e.g. regarding trust. For example the **Shop window - museum - wastebasket** method works by implementing a Security Circle intervention (similar to quality circles) with a group of five to seven employees and a moderator in each functional unit and letting them develop suggestions on how to categorize recent attempts to improve IT security in the organizations. The Shop window category includes successful methods that can be shown to the members of the organizations as very good techniques. The museum-category includes methods that once were successful but are outdated now. Nevertheless, they remind us of "old time" in which they were helpful but would not be useful today anymore. The wastebasket-category includes all methods, measures and techniques that were never helpful and should be thrown in the waste. This can include e.g. inappropriate, extremely laborious and cumbersome actions, rules or regulations. After all, security circles made their categorization, discussing in larger groups with the IT security department, what they think about the category's content. The spotless mind squad should also keep track of all the old routines which are later replaced. This will help in those occasions where old routines come back again. Then the squad will know important cues already and be able to react properly, so "we won't forget what has been (intentionally) forgotten" – and why.

Agents for change: When a new member joins an organization and a team, they often adopt obsolete and insecure behaviors to *fit in*, even if they learned the secure behaviors the organization mandates as part of their induction training. Applying the IF approach (without being aware of it at the time) one of the authors of this paper created a new approach for induction sessions for new joiners in an organization: After introducing the organization's security policies and behaviors (do's and don'ts), they were told in a matter-of-fact way that most teams currently did not follow many of these policies in their day-to-day practice. It was explained that security communications had not been effective, or that policies might not fit existing working practices, so teams had developed coping strategies or *shadow security* practices. This was understandable, but the secure behaviors they had learned needed to be adopted to protect their organization – and it needed the help of the inductees to change behaviors of existing employees. The inductees had "being agents for change" as part of their job description, and all employees were told that new team members had been given the task of clarifying the rules, reminding everyone, and to be the conduit to the IT security team when security policies created friction. The agents had their own network – similar to security champions – to share experiences of embedding security behavior with each other, and the security team.

Habit strength analysis: Based on the empirical results by Roling et al. [80] and Schüffler et al. [84, 85] on the individual level we suggest work analysis methods to identify barriers to forgetting: Organizations need to determine the **habit strength** (how "automated" it is) of an embedded routine that compete with the new secure behavior. The higher the habit storage and retrieval strength, the more effort the forgetting agent team needs to assign to decommissioning it. They need to analyze the changes required for the new IT security routine sequence and categorize them as 1) which action within the sequence is supposed to be not executed anymore, 2) what is executed differently (but the action itself remains, and 3) what is a new action that is added in the sequence of actions. Action from category one is harder to forget and needs more instruction to be forgotten.

Contextual reminders: When employees log in and out, the messages can be displayed reminding them what has changed – what not to do any more, and what to do instead. That sends clear and strong cues (situational strength) to every employee about what the organization expects to be forgotten. Employees benefit from actually seeing both – the old to be forgotten and the new items and elements of an IT security routine. And those messages can be given by team leaders at the start or end of virtual team meetings in the home office scenario.

New look: Design a new and unique desktop layout when unwanted routines should be forgotten so that the execution of that routine is interrupted. This new and unique desktop layout should be designed with high standards on user experience to make the unlearning attractive, because the new routine is more convenient, easier to execute or even with a high aesthetic quality so that employees naturally choose and "want" to use the new instead of the unwanted routine.

Using rewards: Other research mentions that habits are composed of cues, behavior and also rewards. Renaud et al. [77], for example, have created an intervention in which they used longer-lasting passwords as a reward for using a strong password. For this intervention they used a three-part approach, consisting of a simple nudge, the incentive and a reminder. In their discussion they make

it clear that, due to the testing of combinations of interventions, it is not feasible to consider the influence of the individual aspects or their interaction in isolation. What they drew as a conclusion, however, is that the hybrid nudge as a whole was successful because it led to longer and more secure passwords. Becker et al. [48] used the same concept of rewards.

Other small measures to support the switch to password manager would be: remove the notepad from your desk. Remove the icons of the password files from your Desktop. Deleting all obsolete pages from organizations wiki. Autofill password fields and store the passwords in a password manager (e.g. like Apple's Keychain). Don't teach new team members in awareness training about password creation rules. Don't discuss in team meetings how you were organizing your passwords in the past or instruct explicitly to forget these former routines. Replace the keyboards together with the introduction of new password managers. Remove any old technical password routine in any application, like "change your password every 30 days". There are also circumstances that are not conducive to IF, and that organizations should take care to avoid:

Stress and time pressure: Empirical results show that as soon as employees perceive time pressure IF errors increase while they try to recall and execute a new routine. Eliminating the clock and the counter on the desktop or other devices, for the period of time in which a new IT security routine is not well proceduralized and installed as a new routine can help. The perception of a clock already causes employees to speed up or to skip relevant IT security procedures because they feel forced and reminded to be (more) *productive*.

Unclear chain of command: The structure of an organization itself can inhibit IF. Departments may issue different and conflicting rules, so that employees ultimately have to decide on their own which rule to follow. A very illustrative example that has actually occurred is that data privacy officers wanted to enforce the shredding of documents in special closed baskets, while the sustainability office wanted to encourage employees to put all their paper in the paper recycling bin so that it can be reused. So employees were left to decide what was more important and for most, recycling was a stronger routine, so most paper was put into the recycling bin, even when this caused privacy problems. The organization eventually installed paper recycling bins with integrated shredders. CISO's and IT security experts are often too far away from everyday business to know what practices are common in the organization [8] and end up issuing new rules and procedures that conflict with such deeply embedded routines, and that employees can't, or won't, follow. In other cases, rules from different departments might just stack up until they exceed the maximum compliance budgets [12] of employees.

The long shadow of bad security experiences: Employees and teams sometimes internalize routines based on bad experiences with IT security measures. Users that once had problems with updates are likely to deactivate the important auto-update [6]. The arguable concept of fear appeals [52] can also cause users and employees to connect emotions of fear with specific behavior and tools. If you watched a colleague struggle to access files on an encrypted memory stick in front of an impatient client, the memory of that embarrassment will be associated with that memory for a long time [12]. Ashenden & Lawrence [7] report that developers tended not to tell IT security experts about new developments because of past experiences of having projects shut down, and the fear that IT security experts just "kill your baby" had become embedded. IF can help to suppress the knowledge of bad experiences and emotions. Renaud et al. [75] also found that employees often feel shame when they are made responsible for security incidents. Management often foster this shame and it has a negative impact on the employees' work attitude.

Fear of the unknown: Most people don't understand how encryption works [99] and how password managers ensure a high level of security [31]. From other examples we also know that the availability of required data is a strong blocker of new security measures when users assume that the measure can prevent them from easily accessing their data [12]. This can also be assumed for the introduction of password managers. Users might ask "what if something goes wrong?". Therefore, we assume that every IF intervention must be accompanied with the explicit deconstruction of non-applicable hypotheses of IT security measures.

In the case of password managers, it is especially challenging to break routines, because people developed routines as part of coping strategies over decades and used them in organizations and at home. That means that new employees joining teams and organizations with the initial will to use new routines might quickly be overwhelmed with the unwanted routines that can be found everywhere. Here IF is a powerful mechanism that can even remove such established routines. The cues that lead users to prefer a file or note over a password manager must be identified. That can for example be that the Excel icon is always present in the task bar or the notepad lies directly under the display and users associate the filling-in of password fields with these visual cues. After the identification, the cues can be removed and new cues can be established. The introduction of password managers in organizations are in most cases just a single event that is not accompanied by other changes in the daily routine. However, IF explains that the adoption will be hard in case the UI & UX of other applications does not change at all and old cues remain. This suggests that such introduction should be carried out together with other changes (e.g. major updates of the e-mail or browser clients) in order to associate the usage of a password manager with new cues that are introduced either way.

6 Discussion

Many usable security interventions suggested by researchers try to change a specific security behavior of individuals. IF is an organizational design approach that smoothes the path to new behaviors: it acknowledges that a person brings in their routines and over-learned behavioral patterns, which the organizations wants them to forget. It imposes the responsibility for making behavior change possible on the organization, to provide clear implicit and explicit cues and hints for wanted behaviors. A context that creates a situational weakness or strength arises depending on the (un)ambiguousness and (in)consistency of the cues [61]. The example outlined in the previous section shows how organizations unintentionally confuse their employees by asking them to adhere to two conflicting organizational requirements: to 1) shred paper due to security reasons and to 2) simultaneously save paper by

reusing or recycling it. How can employees decide what to do? In such a case, the interplay between person and situational strength can explain why employees differ in behavioral patterns and performance [25] e.g. in applying IT security rules. Brostoff & Sasse [19] argued 20 years ago that security professionals needed to understand which contributing factors and correlated cues mislead employees in executing unwanted routines. IF offers a systematic approach that organizations can use to identify contributing factors (such as cues that trigger unwanted routines, out-of-date knowledge lingering in some documents, employees facing conflicting goals or fearing failure or embarrassment) that need to be tackled at organizational level. It also forces organizations to ensure the security behaviors it demands of its employees are feasible, which in this context means to remove ambiguity and to improve consistency. They are also forced to provide the financial, technical, and time resources needed to embed those behaviors – and finally tackle the fact that security and business processes need to be aligned. The approach encourages solutions that are good for security and productivity: designing your security so it requires a set of unambiguous behaviors, which can be executed in a consistent manner. Leaving employees, who have to process many emails a day, to work out which links are safe to click on, and which are not, will always be an error-prone solution. It is worth working out which of the organization's processes really need embedded links and attachments and to secure the ones that do with available technical measures so a single click by an employee cannot bring down the IT of the entire organization. Systemic issues that may need to be fixed include quality of supervision (e.g. do supervisors plan operation appropriately? Do supervisors themselves violate IT security rules? Do supervisors neglect to fix a problem that employees brought to their attention? Is there a lack of supervision related to the execution of IT security rules?). The precursors leading to the execution of insecure routines (perceived stress, fatigue, sleepiness, inattention, low vigilance) and the design of the routines (slips, lapses, mistakes, violations) themselves.

Future Research Design: Research on unlearning and IF in the last two decades has proven that the approach works in experimental situations[55]. Full empirical validation in organizations is time and resource intensive: the process of forgetting and the implementation of new routines needs at least 28 days. This for changing the behavior of individuals – changing the behavior of whole teams and in organizations might take longer. The research needs to evaluate the progress before, during and after the process of forgetting has been initiated. However, we argue that an extensive study in an organization in the form of an observed intervention is necessary to prove that IF is a proper tool to relieve employees of IT security information overload and improve the secure behavior.

While it might be possible to create an *IF playbook* that works for most organizations (e.g. processes to forget obsolete password policies and routines and management commitment towards the necessity to acknowledge forgetting processes as a part of behavioral change), other IF interventions need to be customized to the requirements of a specific organization. In that case, a first step of any intervention would be to: 1) identify which insecure behavior exists, and which 2) routines are leading to insecure behaviors. Some ideas on how such can be found:

(1) Interviews: Interview employees in order to elicit routines that make sense for the employees, but include security risks from the perspective of the IT department, in order to understand, why those routines are perceived as non-risky. Also interview security experts and managers.
(2) Observation: Observe employees while they are performing their tasks (either by direct observation, or by filming). Document everything.
(3) Technical logs: Log and analyze the user behavior. What applications are used before the insecure routine starts? What other applications are active during the routine? What errors are made?
(4) Diary. Employees should write down what tasks they perform, when and in which order and maybe talk about what they are feeling and thinking during this process.

The identification of the relevant cues is naturally followed by the creation of an appropriate IF measure. In section four, we introduced concrete ideas for supporting the adoption of password managers by removing cues to password routines. Similar interventions could be rolled out for other routines that should be forgotten. The success or failure of the intervention needs to be measured. This can be done with the same techniques that were used to identify the cues in the first place. Here, it needs to be considered that the intervention will typically take at least 28 days till it works. At least one measurement cycle should therefore happen after these 28 days.

IF & Nudging: Nudging is a concept from behavioral economics [92] which has been applied in many areas, including in IT security [76] to encourage the adoption of secure behaviors. Zimmermann & Renaud [100] pointed out that nudging seems to be often misunderstood as a tool that can be applied to make individuals change their behavior towards the secure one. This is missing key points in Thaler & Sunstein's original work – the new behavior has to be easy to execute, i.e. feasible – and aspects subsequently spelt out by Sunstein & Reisch [91]: The individual has to agree they want to change their behavior, and be better off as a result of doing so (as perceived by the individual themselves). These pre-conditions of successful nudging are represented in the security hygiene and concordance stages of our behavior change curve. Nudges themselves are deployed during the embedding stage, where they work in tandem with IF: nudges can remind employees of the new behaviors they are meant to adopt, and why. An IF approach is needed to smooth the path by removing cues that trigger the unwanted old behavior. In our view, the argument for using both in tandem at the final stage of the behavior change curve is compelling, but this still needs to be validated in empirical research studies.

Change Management: While single IF interventions might be used to change the behavior of single employees or teams, it is unlikely to succeed if other behaviors or cues are not aligned. Establishing a set of secure behaviors in your employees requires long-term planning and a joined-up approach to designing work and security behaviors, and supporting behavior change at the individual, team, and organizational level [30, 83]. IF helps the organization to "design out" unwanted cues, but this is only aspect. Change requires effort and resources, while the productivity show

must go on. This means we can initiate change of one or two behaviors at a time, and once they have become routine, embark on the next few – and these must fit with, re-inforce, the previously learned ones. Without a clear long-term goal and plan, a succession of changes that undo each other would be hugely annoying to employees. Schueffler et al. [85] suggested that a change management – such as the change management model according to Kotter [56] – can provide a framework for long-term planning and implementation of behavior change, so each IF intervention can provide a "piece of the puzzle". Furthermore, it must be taken into account that any change to routines creates additional workload, uncertainty, and potentially stress for employees. This is why organizations should only change a few routines at a time, and wait until they have bedded in before introducing more. ITS remains a secondary task for employees and IF could allow employees to adequately deal with the information load so the secondary task becomes easier for them.

Protection Motivation Theory: The Protection Motivation Theory (PMT) is one of many theories used to explain how protective behavior can be initiated and maintained [34]. In addition, PMT is a proven theoretical basis for analyzing recommendations for action or behavior in order to prevent the consequences of hazards [50]. It was originally formulated by Rogers [79] and postulates the following three crucial components: (1) the dimension of the harmfulness of an incident, (2) the probability that the event will occur and (3) the effectiveness of the protective reaction [79]. The threat-appraisal process and the coping-process are the two cognitive processes along which PMT is organized [34]. The threat appraisal consists of the following two components: perceived vulnerability and perceived severity. Coping appraisals are composed of three sub-components: self-efficacy, response efficacy and response cost [47].

PMT was applied to the field of ITS in the context of companies and organizations and was empirically investigated, for example in the studies of [94], who integrated the full PMT model with the Theory of Habit [44, 47, 50, 98]. Overall, applications of PMT in practice have not had long-term success. The reason is that PMT's focus on motivation puts leaves the individual to carry the effort of achieving change, powered by motivation, and not enough on the environment being shaped to smooth the path. We would respectfully suggest that this approach is outdated, given the insights we now have from research on nudges and habits. As BJ Fogg [16] puts it "motivation is not enough" when it comes to achieving behavior change. His behavior model shows of three factors: motivation, ability and triggers. The more effort (ability) the change requires, the higher motivation has to be - and there is a diminishing return the higher it has to be, and the longer it has to be sustained. Fogg argues that the solution to increase behavioral performance cannot be just to increase motivation, but to increase ability. The easier we make the new behavior, the less ability or motivation is required - so making behavior simpler or more feasible is the way forward. This aligns completely with nudge theory – as Thaler recently put it "if you want people to do something, make it easy."[6]

[6]https://www.ft.com/content/a317c302-aa2b-11e9-984c-fac8325aaa04, accessed September 6th 2021

Economic Considerations: It might seem that IF interventions are yet another mechanism for trying to encourage secure behaviors from employees. But we are clear that IF alone will not do that – it is only one element in the acquisition of a new routine. But it is a crucial one: changing policies is cheap; but if existing routines keeping being triggered, employees can't follow suit. IF provides the guidance for making additional investment to change the elements involved in the new policy. The accompanying changes require forethought and planning, but not necessarily great expense. More concrete are some interventions we sketch cheap in terms of monetary cost and required time effort, for example the change of Desktop layouts, the removal of certain sensory cues from desks and offices or the placement of reminders. Those can be implemented without external help or the necessity to buy new products. Workshops, the usage of the *Spotless mind squad* and a habit strength analysis however cost personal resources on the side of the organizers, but also would cost productive time of teams and employees.

Despite the initial costs of the interventions and required change, we think that IF can save resources on the long run, by reducing the security friction leading to more personal productivity loss of the employees and by reducing the number of necessary security measures and rules that need to be used by the employees: IF can function as a workload-reduction. We finally want to mention that even if IF is more costly than simple measures, like generic awareness campaigns, there is at least a good chance that IF really changes the behavior of employees and that the money used for the interventions would not be wasted.

External factors: Employees' behaviors are, of course, not exclusively influenced by their work environment. Employees also use email, passwords etc. in their personal lives - and established routine behaviors. People utilize various routines depending on a particular usability context, but this requires strong signals of the context, and reminders of the correct routines. Conversely, organizations can communicate the benefits that following the secure behaviors it mandates can have for employees personal contexts: for instance, using a VPN has a number security and non-security benefits, and if you use it all the time, it becomes a routine and not a burden.

Limitations: As we stated before, IF has not been tested in the field, so it still needs to be proven that it works in organizations as well as the results from laboratory experiments suggest. In one lab setting it could be shown that not all types of IF intervention (e.g. just removing a cue versus removing a cue and replacing it with a new one) have the same reliable effect [84]. Applied to security behaviors, IF alone will not change behaviors – is not an 'eraser' that can be used to remove unwanted behaviors. Together with nudging, it is a key intervention to support the final stage of the behavior change journey, Implementation. Figure 1 shows that feasibility of the behavior, concordance, self-efficacy and instruction and training need to be in place first. Also, IF needs to be carefully managed: removing, replacing or changing too many objects, concepts or labels at the same time could be unsettling and annoying to employees. Thus, IF needs to part of a long-term change management process, where behaviors to be transformed

are identified, and the IF interventions chosen will remain in place for the foreseeable future.

7 Conclusion

Most organizations today readily sent out security warnings and how to behave to to avoid falling for it. But old advice are rarely explicitly de-commissioned, and the language and cues to old behaviors are left in place. For employees whose main job is not security, the complexity and contradictions are often overwhelming. While most new techniques are intended to replace old behavior, like password manager, 2FA or the usage of VPN in the home office, neither the IT security and usable security research community, nor practitioner did pay any special attention on the question how users and employees could forget their old and insecure behavior with the new one. In this paper we introduced the concept of Intentional Forgetting (IF) to the field of IT security. IF is a well studied technique in the field of organizational psychology that has its origin in learning-unlearning theories. IF offers techniques on how to actively support the suppression of old routines on the level of organizations, teams and individuals. Based on the example of password managers we showed what cues can lead to the refusal of its usage, followed by the introduction of concrete IF techniques that could be used to remove those cues. We argue that IF can help in IT security

(1) by eliminating unwanted routines more efficiently,
(2) by reducing the number of errors when routines change,
(3) by eliminating triggers of unsafe behavior in complete groups and organizations and
(4) by making changes to new routines (new secure measures) possible.

The bigger picture shows that organizations are still struggling to find the right ways to ensure that employees are using security measures as intended and that they do not consider how the repetitive introduction of new and allegedly innovative measures fit into the everyday work. We argue that security awareness training, simulated phishing campaigns, IT security awareness months and tools that might seem usable in theory but do not integrate in the workflow in practice are the wrong ways. Too many threats and potential countermeasures exist for any one to follow along and implement. Hence, organizations need to focus on the most pressing ones. IF is a first piece in a larger picture that aims at "taking out the trash" in the IT security jungle in order to make security usable and practical applicable again.

We are planning on carrying out IF interventions in real organizations in the near future in order to prove that IF can indeed be used like intended. All research needs to be designed in a way that long term changes are observed, meaning that the routines of participants need to be evaluated months or even years after interventions. Any fallback to old routines needs to be reported. Here, we already want to stress that any report about IF research in the field needs to explicitly explain where it did not work. We acknowledge the threat that the success of single IF interventions might to easily be generalized to others.

Acknowledgments

We would like to thank Simon Parkin for his valuable feedback and proofreading. Many thanks to Karen Renaud and Filipo Sharevski for shepherding us through the revisions – like the anonymous reviewers, they provided much constructive criticism and important pointers. We would also like to thank the wonderful NSPW panel which provided so many insightful thoughts, captured by the amazing scribe, which found their way into the final version of this paper. The work was (partially) supported by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federal state of NRW, Germany and also by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972.

References

[1] Nora Alkaldi and Karen Renaud. 2016. Why Do People Adopt, or Reject, Smartphone Password Managers?. In *Proceedings 1st European Workshop on Usable Security*, Karen Renaud and Melanie Volkamer (Eds.). Internet Society, Reston, VA.
[2] Norah AlKaldi and Karen Renaud. 2021. Forthcoming: MIGRANT: Modeling Smartphone Password Manager Adoption using Migration Theory. *The Data Base for Advances in Information Systems* (2021).
[3] T. S. Amer and Jo-Mae B. Maris. 2007. Signal Words and Signal Icons in Application Control and Information Technology Exception Messages—Hazard Matching and Habituation Effects. *Journal of Information Systems* 21, 2 (2007), 1–25.
[4] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. Association for Computing Machinery, Portland, Oregon, USA, 2489–2503.
[5] Anthony Vance, David Eargle, Jeffrey L. Jenkins, C. Brock Kirwan, and Bonnie Brinton Anderson. 2019. The fog of warnings: how non-essential notifications blur with security warnings. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, Santa Clara, CA, USA, 407–420.
[6] Arunesh Mathur and Marshini Chetty. 2017. Impact of user characteristics on attitudes towards automatic mobile application updates. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, Santa Clara, CA, USA, 175–193.
[7] D. Ashenden and D. Lawrence. 2016. Security Dialogues: Building Better Relationships between Security and Business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.
[8] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.
[9] Maria Bada, Angela M. Sasse, and Jason R. C. Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).
[10] Daniel V. Bailey, Markus Dürmuth, and Christof Paar. 2014. Statistics on Password Re-use and Adaptive Strength for Financial Accounts. In *Security and Cryptography for Networks*, Michel Abdalla and Roberto de Prisco (Eds.). Springer International Publishing, Cham, 218–235.
[11] Adam Beautement, Ingolf Becker, Simon Parkin, Kat Krol, and M. Angela Sasse. 2016. Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours. In *Proceedings of the Twelfth USENIX Conference on Usable Privacy and Security (SOUPS '16)*. USENIX Association, USA, 253–270.
[12] Adam Beautement, M. Angela Sasse, and Mike Wonham. 2008. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, Angelos Keromytis, Anil Somayaji, Christian W. Probst, and Matt Bishop (Eds.). Association for Computing Machinery, New York, 47.
[13] M. C. Becker. 2004. Organizational routines: a review of the literature. *Industrial and Corporate Change* 13, 4 (2004), 643–678.
[14] Denis Besnard and Budi Arief. 2004. Computer security impaired by legitimate users. *Computers & Security* 23, 3 (2004), 253–264.
[15] Marcus Beyer, Sarah Ahmed, Katja Doerlemann, Simon Arnell, Simon Parkin, M. Angela Sasse, and Neil Passingham. 2015. 'Awareness is only the first step'. *Hewlett Packard* (12 2015).
[16] BJ Fogg. 2019. *Tiny Habits: The Small Changes that Change Everything*. Houghton Mifflin Harcourt.

[17] Robert A. Bjork. 2011. On the symbiosis of remembering, forgetting, and learning. In *Successful remembering and successful forgetting: A festschrift in honor of Robert A. Bjork*. Psychology Press, New York, NY, US, 1–22.

[18] Robert A. Bjork and Elizabeth Ligon Bjork. 1992. A new theory of disuse and an old theory of stimulus fluctuation. In *Essays in honor of William K. Estes, Vol. 1: From learning theory to connectionist theory; Vol. 2: From learning processes to cognitive processes*. Lawrence Erlbaum Associates, Inc, Hillsdale, NJ, US, 35–67.

[19] Sacha Brostoff and M. Angela Sasse. 2001. Safe and sound: A safety-critical approach to security. In *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW '01)*, Victor Raskin (Ed.). ACM, New York, NY, 41.

[20] Bundesamt für Sicherheit in der Informationstechnik. 2021. IT-Sicherheit im Home-Office (German).

[21] Tristan Caulfield and Simon Parkin. 2016. Case study: predicting the impact of a physical access control intervention. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. Association for Computing Machinery, Los Angeles, California, 37–46.

[22] Michael D. Cohen and Paul Bacdayan. 1994. Organizational Routines Are Stored as Procedural Memory: Evidence from a Laboratory Study. *Organization Science* 5, 4 (1994), 554–568.

[23] Lizzie Coles-Kemp, Rikke Bjerg Jensen, and Claude P. R. Heath. 2020. Too Much Information: Questioning Security in a Post-Digital Society. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14.

[24] Lynne Coventry, Pam Briggs, Debora Jeske, and Aad van Moorsel. 2014. SCENE: A Structured Means for Creating and Evaluating Behavioral Nudges in a Cyber Security Environment. In *Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience*, Aaron Marcus (Ed.). Springer International Publishing, Cham, 229–239.

[25] Reeshad S. Dalal, Devasheesh P. Bhave, and John Fiset. 2014. Within-Person Variability in Job Performance. *Journal of Management* 40, 5 (2014), 1396–1436.

[26] A. Demjaha, T. Caulfield, M. Angela Sasse, and D. Pym. 2019. 2 Fast 2 Secure: A Case Study of Post-Breach Security Changes. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 192–201.

[27] Paul Dourish, Rebecca E. Grinter, Jessica La Delgado de Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[28] Thomas Ellwart and Annette Kluge. 2019. Psychological Perspectives on Intentional Forgetting: An Overview of Concepts and Literature. *KI - Künstliche Intelligenz* 33, 1 (2019), 79–84.

[29] ENISA. 16.04.2019. Behavioural aspects of cybersecurity.

[30] ENISA. 2018. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.

[31] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. 2017. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences* 7, 1 (2017).

[32] Michael Fagan and Mohammad Maifi Hasan Khan. 2016. Why Do They Do What They Do? A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Proceedings of SOUPS 2016, Twelfth Symposium on Usable Privacy and Security*. USENIX Association, Berkeley, CA, 59–75.

[33] F. M. Farke, L. Lorenz, T. Schnitzler, P. Markert, and M. Dürmuth (Eds.). 2020. *"You still use the password after all" - Exploring FIDO2 Security Keys in a Small Company*.

[34] Donna L Floyd, Steven Prentice-Dunn, and Ronald W Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of applied social psychology* 30, 2 (2000), 407–429.

[35] Muriel Frank and Vanessa Kohn. 2021. How to Mitigate Security-Related Stress: The Role of Psychological Capital. In *Proceedings of the 54th Hawaii International Conference on System Sciences (Proceedings of the Annual Hawaii International Conference on System Sciences)*, Tung Bui (Ed.). Hawaii International Conference on System Sciences.

[36] Steven Furnell. 2005. Why users cannot use security. *Computers & Security* 24, 4 (2005), 274–279.

[37] Brian Glass, Graeme Jenkinson, Yuqi Liu, Angela Sasse, and Frank Stajano. 2016. The usability canary in the security coal mine: A cognitive framework for evaluation and design of usable authentication solutions.

[38] Maximilian Golla and Markus Dürmuth. 2018. On the Accuracy of Password Strength Meters. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang (Eds.). ACM, New York, NY, USA, 1567–1582.

[39] Thomas Grisold, Alexander Kaiser, and Julee Hafner. 2017. Unlearning before Creating new Knowledge: A Cognitive Process. In *Proceedings of the 50th Hawaii International Conference on System Sciences (2017) (Proceedings of the Annual Hawaii International Conference on System Sciences)*. Hawaii International Conference on System Sciences.

[40] Jennifer Haase, Julia Matthiesen, Arnulf Schueffler, and Annette Kluge. 2020. Retentivity Beats prior Knowledge as Predictor for the Acquisition and Adaptation of New Production Processes. In *Proceedings of the 53rd Hawaii International Conference on System Sciences (Proceedings of the Annual Hawaii International Conference on System Sciences)*, Tung Bui (Ed.). Hawaii International Conference on System Sciences.

[41] Christopher Hadnagy. op. 2011. *Social engineering: The art of human hacking*. Wiley Publishing, Inc, Indianapolis.

[42] Hana Habib, Pardis Emami-Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2018. User behaviors and attitudes under password expiration policies. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, Baltimore, MD, USA, 13–30.

[43] Chip Heath and Dan Heath. 2010. *Switch: How to change things when change is hard*. Broadway Books, New York.

[44] Tejaswini Herath and H Raghav Rao. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems* 18, 2 (2009), 106–125.

[45] Cormac Herley and Paul van Oorschot. 2012. A Research Agenda Acknowledging the Persistence of Passwords. *IEEE Security Privacy* 10, 1 (2012), 28–36.

[46] Donald Hislop, Sara Bosley, Crispin R. Coombs, and Julie Holland. 2014. The process of individual unlearning: A neglected topic in an under-researched field. *Management Learning* 45, 5 (2014), 540–560.

[47] Princely Ifinedo. 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security* 31, 1 (2012), 83–95.

[48] Ingolf Becker, Simon Parkin, and M. Angela Sasse. 2018. The Rewards and Costs of Stronger Passwords in a University: Linking Password Lifetime to Strength. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 239–253.

[49] ISF. 2014. From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance.

[50] Allen C Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: An empirical study. *MIS quarterly* (2010), 549–566.

[51] Daniel Kahneman. 2011. *Thinking, Fast and Slow* (first edition ed.). Farrar Straus and Giroux, Farrar, Straus and Giroux.

[52] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*. Association for Computing Machinery, San Carlos, Costa Rica, 42–56.

[53] Iacovos Kirlappos, Simon Parkin, and M. Angela Sasse. 2014. Learning from "Shadow Security": Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. In *Proceedings 2014 Workshop on Usable Security*, Matthew Smith and David Wagner (Eds.). Internet Society, Reston, VA.

[54] Annette Kluge and Norbert Gronau. 2018. Intentional Forgetting in Organizations: The Importance of Eliminating Retrieval Cues for Implementing New Routines. *Frontiers in psychology* 9 (2018), 51.

[55] Annette Kluge, Arnulf Sebastian Schüffler, Christof Thim, Jennifer Haase, and Norbert Gronau. 2019. Investigating unlearning and forgetting in organizations. *The Learning Organization* 26, 5 (2019), 518–533.

[56] John P. Kotter. 2011. *Leading Change: Wie Sie Ihr Unternehmen in acht Schritten erfolgreich verändern*. Verlag Franz Vahlen, München.

[57] L. Zhang-Kennedy, S. Chiasson, and P. van Oorschot. 2016. Revisiting password rules: facilitating human management of passwords. In *2016 APWG Symposium on Electronic Crime Research (eCrime)*. 1–10.

[58] C. Maasdorp and N. and Gronau. 2016. Modeling of Organizational Knowledge and Information.

[59] Steve J. Martin, Noah J. Goldstein, and Robert B. Cialdini. 2015. *The small BIG: Small changes that spark BIG influence*. Profile Books, London.

[60] Pablo Martin de Holan. 2011. Agency in Voluntary Organizational Forgetting. *Journal of Management Inquiry* 20, 3 (2011), 317–322.

[61] Rustin D. Meyer, Reeshad S. Dalal, and Richard Hermida. 2010. A Review and Synthesis of Situational Strength in the Organizational Sciences. *Journal of Management* 36, 1 (2010), 121–140.

[62] Susan Michie, Maartje M. van Stralen, and Robert West. 2011. The behaviour change wheel: a new method for characterising and designing behaviour change interventions. *Implementation science : IS* 6 (2011), 42.

[63] Frederick P. Morgeson, Terence R. Mitchell, and Dong Liu. 2015. Event System Theory: An Event-Oriented Approach to the Organizational Sciences. *Academy of Management Review* 40, 4 (2015), 515–537.

[64] Nissy Sombatruang, M. Angela Sasse, and Michelle Baddeley. 2016. Why do people use unsecure public wi-fi? an investigation of behaviour and factors driving decisions. In *Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust*. Association for Computing Machinery, Los Angeles, California, 61–72.

[65] Palo Alto Network. 2021. The State of Hybrid Workforce Security 2021 - Whitepaper.

[66] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, Santa Clara, CA, USA, 319–338.

[67] Brian T. Pentland and Thorvald Hærem. 2015. Organizational Routines as Patterns of Action: Implications for Organizational Behavior. *Annual Review of*

Organizational Psychology and Organizational Behavior 2, 1 (2015), 465–487.
[68] Paul B. Perrin, Bruce D. Rybarczyk, Bradford S. Pierce, Heather A. Jones, Carla Shaffer, and Leila Islam. 2020. Rapid telepsychology deployment during the COVID-19 pandemic: A special issue commentary and lessons from primary care psychology training. *Journal of Clinical Psychology* 76, 6 (2020), 1173–1185.
[69] Martin Prinz and Tobias Seitz. 2017. *Towards a Mental Model of Password Management Software.*
[70] R. W. Reeder, I. Ion, and S. Consolvo. 2017. 152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users. *IEEE Security & Privacy* 15, 5 (2017), 55–64.
[71] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis, and C. Peersman. 2019. *The Cyber Security Body of Knowledge* (1 ed.). The National Cyber Security Centre.
[72] J. T. Reason. 1990. *Human error.* Cambridge University Press, Cambridge [England] and New York.
[73] J. T. Reason. 2016. *The human contribution: Unsafe acts, accidents and heroic recoveries.* Routledge, London.
[74] Robert Reeder and Stuart Schechter. 2011. When the Password Doesn't Work: Secondary Authentication for Websites. *IEEE Security Privacy* 9, 2 (2011), 43–49.
[75] Karen Renaud, Rosalind Searle, and Marc Dupui. 2021. Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?. In *To appear in: Proceedings of the 2021 Workshop on New Security Paradigms.* Association for Computing Machinery, New York.
[76] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35.
[77] Karen Renaud and Verena Zimmermann. 2019. Nudging folks towards stronger password choices: providing certainty is the key. *Behavioural Public Policy* 3, 2 (2019), 228–258.
[78] Hyeun-Suk Rhee, Cheongtag Kim, and Young U. Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security* 28, 8 (2009), 816–826.
[79] Ronald W Rogers. 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology* 91, 1 (1975), 93–114.
[80] Wiebke Roling, Arnulf Schüffler, Christof Thim, Norbert Gronau, and Annette Kluge. 2021. *Der Einfluss von Zeitdruck auf das willentliche Vergessen veralteter Produktionsroutinen.*
[81] M. A. Sasse, S. Brostoff, and D. Weirich. 2001. Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* 19, 3 (2001), 122–131.
[82] M. Angela Sasse, Michelle Steves, Kat Krol, and Dana Chisnell. 2014. The Great Authentication Fatigue – And How to Overcome It. In *Cross-Cultural Design*, P. L. Patrick Rau (Ed.). Springer International Publishing, Cham, 228–239.
[83] Thomas Schlienger. 2006. *Informationssicherheitskultur in Theorie und Praxis - Analyse und Förderung sozio-kultureller Faktoren der Informationssicherheit in Organisationen.* Ph.D. Dissertation.
[84] Arnulf Schüffler, Christof Thim, Jennifer Haase, Norbert Gronau, and Annette Kluge. 2019. Willentliches Vergessen – Voraussetzung für Flexibilität und Veränderungsfähigkeit in einer sich permanent verändernden Welt. *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie (GIO)* 50, 2 (2019), 197–209.
[85] Arnulf Sebastian Schüffler, Christof Thim, Jennifer Haase, Norbert Gronau, and Annette Kluge. 2019. Information Processing in Work Environment 4.0 and the Beneficial Impact of Intentional Forgetting on Change Management. *Zeitschrift für Arbeits- und Organisationspsychologie A&O* 64, 1 (2019), 17–29.
[86] Tobias Seitz. 2018. Supporting users in password authentication with persuasive design (Dissertation).
[87] Nissy Sombatruang, Tan Omiya, Daisuke Miyamoto, M. Angela Sasse, Youki Kadobayashi, and Michelle Baddeley. 2020. Attributes Affecting User Decision to Adopt a Virtual Private Network (VPN) App. In *Information and Communications Security*, Weizhi Meng, Dieter Gollmann, Christian D. Jensen, and Jianying Zhou (Eds.). Springer International Publishing, Cham, 223–242.
[88] Sabine Sonnentag, Wilken Wehrt, Benjamin Weyers, and Yuen Law. 2019. Conquering unwanted habits at the workplace: A daily-survey approach. *Academy of Management Proceedings* 2019 (2019), 12420.
[89] Michelle Steves, Dana Chisnell, Angela Sasse, Kat Krol, Mary Theofanos, and Hannah Wald. 2014. Report: Authentication Diary Study.
[90] Elizabeth Stobert and Robert Biddle. 2014. A Password Manager that Doesn't Remember Passwords. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop - NSPW '14*, Konstantin Beznosov, Anil Somayaji, Tom Longstaff, and Paul van Oorschot (Eds.). ACM Press, New York, New York, USA, 39–52.
[91] Cass R. Sunstein and Lucia A. Reisch. 2019. *Trusting Nudges: Toward a Bill of Rights for Nudging.* Routledge, Milton.
[92] Richard H. Thaler and Cass R. Sunstein. 2009. *Nudge: Improving decisions about health, wealth, and happiness* (rev. and expanded ed., with a new afterword and a new chapter ed.). Penguin, New York, NY.
[93] Walter Ulmer, JR. 2017. *A Military Leadership Notebook: Principles Into Practice.* iUniverse.
[94] Anthony Vance, Mikko Siponen, and Seppo Pahnila. 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management* 49, 3-4 (2012), 190–198.
[95] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing Simulated Phishing Campaigns for Staff. In *Computer Security*, Ioana Boureanu, Constantin Catalin Dragan, Mark Manulis, Thanassis Giannetsos, Christoforos Dadoyan, Panagiotis Gouvas, Roger A. Hallman, Shujun Li, Victor Chang, Frank Pallas, Jörg Pohle, and Angela Sasse (Eds.). Springer International Publishing, Cham, 312–328.
[96] Wei Miranda, Golla Maximilian, and Ur Blase. 2018. The Password Doesn't Fall Far: How Service Influences Password Choice. In *Who Are You?! Adventures in Authentication Workshop (WAY '18).* USENIX, Baltimore, Maryland, USA.
[97] Alma Whitten and J. D. Tygar. 1999. Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In *Proceedings of the 8th conference on USENIX Security Symposium - Volume 8.* USENIX Association, Washington, D.C., 14.
[98] Michael Workman, William H Bommer, and Detmar Straub. 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior* 24, 6 (2008), 2799–2816.
[99] Justin Wu and Daniel Zappala. 2018. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security (SOUPS '18).* USENIX Association, USA, 395–409.
[100] Verena Zimmermann and Karen Renaud. 2021. The Nudge Puzzle: Matching Nudge Interventions to Cybersecurity Decisions. *ACM Trans. Comput.-Hum. Interact.* 28, 1, Article 7 (Jan. 2021), 45 pages.