Taking out the Trash:

Why Security Behaviour Change requires Intentional Forgetting

Jonas Hielscher, Uta Menges, M. Angela Sasse & Annette Kluge

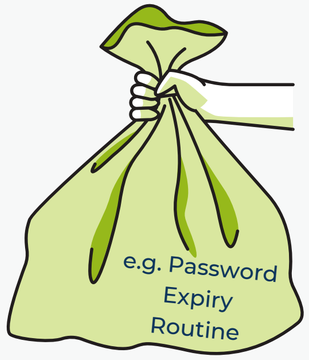
LEHRSTUHL AOW
ARBEITS.ORGANISATIONS.WIRTSCHAFTSPSYCHOLOGIE

HCS

RUB

Security Awareness is not enough

Security Awareness alone is not enough for employees to replace old insecure routines with new secure ones. One significant blocker is the missing disabling of existing (insecure) routines – the failure to take out the trash – that prevents embedding of new (secure) routines. Organizational Psychology offers the paradigm *Intentional Forgetting (IF)* and associated tools for replacing old behavior. In our paper (Hielscher et al. 2021) we explain which steps are necessary to enable secure routines and outline how IF could be applied in the security realm:



1. Security Hygiene

Security measures should be subjected to a feasibility check, as complex and effortful routines cannot be enbedded. They must be within the *Compliance Budget*.

2. Establishing Concordance

Behavior change is more likely when employees can commit to the goals and agree on the steps to reach those goals.

3. Enabling self-efficacy

Employees need to have confidence in their own ability to succeed, through direct or vicarious experience (ENISA 2018).

4. Implementation

While the new behavior is becoming proceduralized, employees need to be reminded that and why they are choosing the new secure behavior.

5. Embedding: Intentional Forgetting

IF is an organizational design approach. It works by replacing or removing so-called cues that are associated with the execution of a routine (the respective memory element) (Kluge & Gronau 2018). IF can be applied on individual, team, or even organisational level.

Four cue types (Kluge & Gronau 2018):

1. **Sensory cues** (names, icons, graphics, sounds etc.)
2. **Routine-related cues** (actor-related, object-related cues etc.)
3. **Time and space cues** (stimuli indicating location and time)
4. **Situational strenght cues** (implicit or explicit cues provided by external entities)

Implementation of IF in IT Security - VPN

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. It can be combinded with an auditory cue.

Conclusion

IF is a first piece in a larger picture that aims at "taking out the trash" in the IT security jungle (Reeder et al. 2017), making security usable and practical.

Scan to go to the article

[1] Hielscher, Jonas; Kluge, Annette; Menges, Uta; Sasse, M. Angela (2021): "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. In: New Security Paradigms Workshop. NSPW '21
[2] ENISA- European Union Agency for Network and Information Security (2019): Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity
[3] Kluge, Annette; Gronau, Norbert (2018): Intentional Forgetting in Organizations: The Importance of Eliminating Retrieval Cues for Implementing New Routines. In: Frontiers in psychology
[4] Reeder, Robert; Ion, Iulia; Consolvo, Sunny (2017): 152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users. In: IEEE Secur. Privacy
The work was supported by the PhD School "SecHuman - Security for Humans in Cyberspace" by the federalstate of NRW.

SecHUMAN
FORSCHUNGSKOLLEG
SECURITY FOR HUMANS IN CYBERSPACE