**Study Information**

1. Title (required)

Exploring Augmented Reality Interventions for Enhancing Cybersecurity Self-Efficacy and Calibrating Symbol Trust in the Context of Smart Home Technologies

2. Authors (required)

Removed for anonymization

3. Description (optional)

Though there are some interventions aimed at increasing cybersecurity self-efficacy (Borgert et al., 2023), none has neither (a) singled out distinguishing effects of the different, theoretically underlying sources of self-efficacy, nor (b) investigated the specific context of smart home technologies, nor (c) used Augmented Reality (AR) as an educational tool. Therefore, we designed three AR interventions that all focus on the visualization of privacy and IT security within smart home data flow structures but differ in their main approach to foster self-efficacy beliefs through addressing different sources. Emotional arousal was not included as an intervention, given its posited rather unreliable nature (Bandura, 1977; 1986). Instead, we added an intervention that primarily manipulates an assumed overtrust in specific, disadvantageous device settings. The relationship between trust and self-efficacy is conceptually based in the framework of the Self-Determination Theory (Deci & Ryan, 1985). This study uses a Solomon design with the following groups:

• Default control group (post only): mastery experience only

• Default intervention A (pre-post): mastery experience only

• Intervention B (pre-post): mastery experience & visual persuasion

• Intervention C (pre-post): mastery experience & vicarious experience

• Intervention D (pre-post): mastery experience & risk uncertainty

4. Hypotheses (required)

**• Pretest sensitization: robust Bayesian estimation for comparing two groups**

o When comparing group A and the CG, the posterior distribution on the effect size of self-efficacy suggests equivalence.

**• Additive and/or restricted self-efficacy effect: regression model**

o Post-intervention self-efficacy is higher in group C and B than in group A.

o Post-intervention self-efficacy is higher in group C than in group B.

**• Effect of trust on self-efficacy: regression model**

o Post-intervention self-efficacy is higher in group D than in group A.

**Design Plan**

5. Study type (required)

Other: interventional study

6. Blinding (required)

Study subjects and personnel who interact directly with study subjects will not be aware of the assigned treatments. (double blind)

7. Is there any additional blinding in this study?

No

8. Study design (required)

This study uses a Solomon design with all groups receiving an intervention. We will employ a pre- and post-measurement of some variables (self-efficacy, perceived knowledge, and tested knowledge) across group A, B, C, and D, whereas group CG will only have a post-measurement phase. Additional post-measurement variables are: systems trust, symbol trust, attitude towards safety, and demographics. Other variables will be measured during the intervention phase (reaction time to the risk-symbol, total completion time, number of successful task completions, and total number of clicks). The CG group and group A will receive the same default intervention (mastery experience only). Interventions of group B (mastery experience & visual persuasion) and C (mastery experience & vicarious experience) involve additional sources of self-efficacy. Group D’s intervention (mastery experience & risk uncertainty) also includes a manipulation on the level of symbol trust.

9. Randomization (optional)

We will use block randomization, where each participant will be randomly assigned to one of the five equally sized, predetermined blocks (A, B, C, D, CG). The random number list used to create these five blocks will be created using the web applications available at <http://random.org>. Within each measurement point, scales will be randomized as well as the items within each scale.

**Sampling Plan**

10. Existing data (required)

Registration prior to creation of data: As of the date of submission of this research plan for preregistration, the data have not yet been collected, created, or realized.

11. Explanation of existing data (optional)

Some data was collected prior to the registration across two pre-studies. This data was used to check the materials of the study with regard to their difficulty and comprehensibility. For the first pre-study, we recruited cybersecurity experts and asked them whether the tested knowledge items are comprehensible and correct in content as well as whether important sub-topics of cybersecurity and privacy in smart homes are still missing. The second pre-study was run on Prolific with a German speaking sample to test made translations, adjustments, and especially item difficulty of the tested knowledge scale. Additionally, each experiment supervisor will run at least one test trial prior to data collection.

12. Data collection procedures (required)

Participants will be recruited through online advertisements (e.g., social media, job platforms) and local advertisements (e.g., flyers, posters, direct marketing). Participants will be paid about €15 (depending on local currencies) or, if they are students, they can choose to be rewarded with a one hour participation credit for their study curriculum. Rewards and advertisement strategies may change if our sample size is not reached timely. Participants must be at least 18 years old, have good German language skills, and must not be affected by severe vision loss because they will have to use the AR app during the study.

13. Sample size (required)

Our target sample size is 500 participants. We will attempt to recruit up to 550, assuming that not all will complete the study or that some may experience technical issues.

14. Sample size rationale (optional)

We used a precision analysis run in R (R version 4.2.2; MBESS package version 4.9.2) to determine the width of a confidence interval around estimated effect sizes (all lower medium effects) for the hypotheses. The script of the performed analyses is attached. Using n = 100 per group in a two group comparison, a confidence interval width of 0.56 (0.28 either side of the point estimate delta = 0.5) would be achieved. Comparing three out of five groups, again using n = 100 per group, a confidence interval width of 0.48 (0.24 either side of the point estimate lambda = 0.25) would be achieved. Applying the same criteria, but comparing two out of five groups, a confidence interval width of 0.56 (0.28 either side of the point estimate lambda = 0.25) would be achieved. To achieve higher precision more participants would be needed. This is not possible given we possess only restricted time and monetary resources for this study.

15. Stopping rule (optional)

We will increase recruitment efforts (or potentially participation rewards) as long as we are below our target sample size. Due to time constraints, we will stop recruitment on 31.12.24 at the latest. Otherwise, we will stop recruitment when the target sample size of N = 550 is reached.

**Variables**

16. Manipulated variables (optional)

We manipulate the sources of self-efficacy and the level of trust. For self-efficacy, the default intervention (mastery experience only) is the use of an augmented reality app that shows you - via the completion of privacy tasks - dataflow consequences of different security behaviors within a smart home environment. Mastery experience revolves around one’s own performance accomplishments and can be induced by self-modeling, performance desensitization, performance exposure, or self-instructed performance. The privacy tasks are categorized as either “easy” (4 tasks) or “difficult” (4 tasks). Thus, we have a pool of 8 total tasks. For each participant, the app draws 1 introductory easy task, then 2 random easy tasks and another 2 random difficult tasks. A second source of self-efficacy we manipulate is visual persuasion (intervention B). This is done by presenting statements in the app that reward the user for taking the right steps towards completing the privacy tasks. According to self-efficacy theory, persuasion can be achieved through suggestion, exhortation, interpretive treatments, or self-instruction. And the third source of self-efficacy we manipulate is vicarious experience (intervention C). Vicarious experience is defined as observing other people perform a behavior of interest, e.g. via live or symbolic modeling. This is induced by providing introductory videos on how to solve the privacy tasks to guide app users.

17. Measured variables (required)

**Pre-post measures:**

• Self-efficacy (CySESH; Borgert et al., 2023): 7-point Likert scale (1=kann ich mit hoher Gewissheit tun, 4=kann ich mit mittelgroßer Gewissheit tun, 7=kann ich mit hoher Gewissheit überhaupt nicht tun); self-translation to German

1. Ich kann die Datenschutzrichtlinien von Geräten zur Risikobewertung hinsichtlich meiner Privatsphäre nutzen.

2. Ich kann die in einer Cloud gespeicherten Daten löschen, wenn ich meine Geräte nicht mehr nutzen möchte.

3. Ich kann die Informationen beschaffen, die ich brauche, um meine gespeicherten Daten auf meinen Geräten zu löschen.

4. Ich kann herausfinden, welche Drittanbieter Zugriff auf die von meinen Geräten gesammelten Daten haben.

5. Ich kann herausfinden, welche Daten meine Geräte sammeln.

6. Ich kann mir das technische Wissen aneignen, um die technischen Datenblätter meiner Geräte zu verstehen.

7. Ich kann die Auswirkungen auf meine Privatsphäre überblicken, wenn ich mehrere Geräte miteinander verbinde.

8. Ich kann erkennen, wenn Benutzeroberflächen so gestaltet sind, dass sie meine Entscheidungen über Sicherheitsoptionen beeinflussen.

9. Ich kann Verletzungen meiner Datenschutzrechte durch eine Gerätefunktion erkennen.

10. Ich kann bei Bedarf Kontakt mit dem Datenschutzbeauftragten eines Herstellers aufnehmen.

11. Ich kann vor dem Kauf eines neuen Geräts Informationen über die damit verbundenen Auswirkungen auf die Privatsphäre einholen.

12. Ich kann meine Geräte im Falle eines Sicherheitsangriffs deaktivieren.

• Perceived knowledge (De Kimpe et al. 2021; Eurobarometer, 2020): 4-point Likert scale (sehr gut informiert; ziemlich informiert; nicht sehr gut informiert; überhaupt nicht informiert); “the internet” replaced with “smart home devices”; self-translation to German

1. Ich fühle mich ausreichend über die Risiken von Smart Home-Geräten informiert.

2. Ich fühle mich ausreichend darüber informiert, wie man die Risiken von Smart-Home-Geräten vermeiden kann.

• Tested knowledge (self-developed and validated in pre-studies): multiple choice; multiple response items

1. Welche der folgenden Daten können grundsätzlich von Smart-Home-Geräten erfasst werden?

o Gerätenutzungsmuster (r)

o Audioaufnahmen (r)

o Suchanfragen (r)

o Keine der anderen Optionen trifft zu.

2. Wozu dient eine Datenschutzerklärung im Zusammenhang mit Smart-Home-Geräten?

o Um die Produktionskosten des Geräts für die Verbraucher\*innen offenzulegen

o Um den Energieverbrauch des Geräts darzustellen

o Um Benutzer\*innen über Datennutzungspraktiken zu informieren (r)

o Um Verwender\*innen mitzuteilen, welche Daten gespeichert werden (r)

3. Welche der folgenden Aussagen treffen auf die Erhebung personenbezogener Daten durch Smart-Home-Geräte zu?

o Smart-Home-Geräte dürfen ohne Einwilligung der Nutzer\*innen personenbezogene Daten sammeln.

o Smart-Home-Geräte erfassen grundsätzlich keine personenbezogenen Daten.

o Nach Zustimmung zur Datenschutzerklärung können Smart-Home-Geräte personenbezogene Daten ihrer Nutzer\*innen sammeln. (r)

o Smart-Home-Geräte erfassen personenbezogene Daten nur, wenn Nutzer\*innen dies ausdrücklich anfordert.

4. Welche potenziellen Risiken birgt die Verwendung von Smart-Home-Geräten im Hinblick auf Datenschutz?

o Unbefugter Zugriff auf personenbezogene Daten (r)

o Physische Schäden an den Geräten

o Höherer Energieverbrauch

o Eingeschränkte Gerätefunktionalität

5. Wie können Benutzer\*innen ihre Daten vor dem Zugriff Unbefugter bei der Verwendung von Smart-Home-Geräten schützen?

o Durch Überprüfung und Anpassung der Datenschutzeinstellungen des Geräts (r)

o Durch regelmäßige Aktualisierung von Firmware und Software, um die Sicherheitsmaßnahmen aktuell zu halten (r)

o Nur die Hersteller können den Datenzugriff kontrollieren.

o Durch Kauf von Smart-Home-Geräten, die Privatsphäre und Datenschutz der Benutzer\*innen priorisieren (r)

6. Was versteht man im Zusammenhang mit Datenverkehr unter „lokaler Verarbeitung“ bei Smart-Home-Geräten?

o Die Daten werden direkt auf dem Gerät verarbeitet und analysiert, ohne an die Cloud gesendet zu werden. (r)

o Die Daten werden vorübergehend auf dem Gerät gespeichert und periodisch stapelweise in der Cloud verarbeitet.

o Die Daten werden von den Servern des Geräteherstellers verarbeitet, bevor sie lokal an das Gerät zurückgesendet werden.

o Die Daten werden an die lokale Verarbeitungsanlage des Herstellers im Aufenthaltsland des Benutzers gesendet.

7. Welche Aussagen über Updates treffen in Bezug auf Smart-Home-Geräte zu?

o Veraltete Firmware könnte Hackern Zugang zu Smart-Home-Geräten geben. (r)

o Alle Smart-Home-Geräte installieren Updates automatisch.

o Eine regelmäßige Aktualisierung von Firmware und Software von Smart-Home-Geräten ist aus Datenschutzgründen nicht erforderlich.

o Die Verfügbarkeit von Softwareupdates muss unabhängig vom Gerät regelmäßig manuell überprüft werden.

8. Welche Aussagen über den Zugriff auf Smart-Home-Geräte von außen treffen zu?

o Der Einsatz eines VPN kann die Sicherheit des Systems bei Remote-Verbindungen erhöhen. (r)

o Durch die Einrichtung verschiedener Benutzertypen wird das System weniger anfällig für Angriffe von außen.

o Um die Sicherheit einer Verbindung zu gewährleisten, empfiehlt sich die Verwendung verifizierter Signaturen. (r)

o Es ist beinahe unmöglich, ohne physischen Zugriff auf Daten in Smart-Home-Systemen zuzugreifen.

9. Welche Aussagen über Sicherheitsmaßnahmen in Bezug auf Smart Homes treffen zu?

o Ohne Authentifizierungsmaßnahmen (wie z. B. Passwörter) können unbeaufsichtigte Gäste auf dieselben Informationen zugreifen wie der Administrator. (r)

o Der beste Weg, ein Passwort festzulegen, besteht darin, es lang und komplex zu machen und dessen Einprägsamkeit vollkommen außen vor zu lassen.

o Die Datenverschlüsselung ist eine wichtige Maßnahme bei Smart-Home-Geräten, um Daten während der Übertragung zu sichern. (r)

o Daten, die von Smart-Home-Geräten an die Cloud übertragen werden, werden niemals verschlüsselt.

10. Welche Aussagen über Datenströme in Smart-Home-Systemen treffen zu?

o Smart-Home-Geräte können Daten sammeln und zur Speicherung und Analyse an die Cloud übertragen. (r)

o Unter lokaler Verarbeitung in Smart-Home-Geräten versteht man die Übertragung von Daten zur Analyse in die Cloud.

o Die Abgrenzung des Heimnetzwerks vom Internet hat keine Auswirkungen auf den Datenschutz der Smart-Home-Geräte.

o Smart-Home-Geräte können für erweiterte Funktionen Daten mit Diensten oder Apps von Drittanbietern teilen. (r)

11. Welche Aussagen über Rechte und Pflichten von Nutzer\*innen und Herstellern treffen in Bezug auf Smart-Home-Geräte zu?

o Benutzer\*innen haben keine Kontrolle über die Anpassung der Datenschutzeinstellungen in Smart-Home-Geräten.

o Von Smart-Home-Geräten erfasste Daten werden stets unbegrenzt gespeichert, ohne Ablauf- oder Löschmechanismen.

o Datenschutzverletzungen in Smart-Home-Systemen können für die Gerätehersteller auch rechtliche Konsequenzen haben. (r)

o Einige Hersteller konzipieren Smart-Home-Geräte so, dass sie Zugriff auf möglichst viele Daten erhalten. (r)

**During-app-use measures:**

• Completion time

• Reaction time to risk symbol

• Number of successful task completions

• Number of clicks

**Post measures:**

• Security attitudes (SA-6; Faklaris et al., 2019): 5- point Likert scale (1=stimme überhaupt nicht zu, 5=stimme voll und ganz zu); self-translation to German

1. Ich bin stets bestrebt, Gelegenheiten zu finden, um mehr über die für mich relevanten Sicherheitsmaßnahmen zu erfahren.

2. Ich bin äußerst motiviert, alle notwendigen Schritte zu unternehmen, um meine Online-Daten und -Konten zu schützen.

3. Im Allgemeinen folge ich gewissenhaft einer Routine bezüglich Sicherheitsmaßnahmen.

4. Ich interessiere mich oft für Artikel über Sicherheitsbedrohungen.

5. Ich höre immer auf den Rat von Expert\*innen, welche Schritte ich ergreifen muss, um meine Online-Daten und -Konten zu schützen.

6. Ich habe äußerst umfassende Kenntnisse über alle erforderlichen Schritte, um meine Online-Daten und -Konten zu schützen.

• System trust (trust in automation scale; Jian et al., 2000): German translation by Beggiato (2015); 7- point Likert scale (1=”stimme überhaupt nichts zu”, 7=”stimme vollkommen zu”); “System” will be changed to “App”

1. Ich kann der App vertrauen.

2. Die App ist irreführend. (-)

3. Die Aktionen der App sind undurchsichtig. (-)

4. Ich misstraue den Aktionen, Absichten oder Konsequenzen der App. (-)

5. Ich bin der App gegenüber wachsam. (-)

6. Ich bin mit der App vertraut.

7. Die Aktionen der App führen zu nachteiligen oder schädlichen Konsequenzen. (-)

8. Ich traue mir zu, die App zu nutzen.

9. Die App ist glaubwürdig.

10. Ich kann mich auf die App verlassen.

11. Die App bietet Sicherheit.

12. Die App ist zuverlässig.

• Symbol trust (FOST scale; Franke et al., 2015): German translation by Trommler et al. (2018); 6- point Likert scale (1=stimmt gar nicht, 2=stimmt weitgehend nicht, 3=stimmt eher nicht, 4=stimmt eher; 5=stimmt weitgehend; 6=stimmt völlig); “Information/System” will be changed to “Symbol”

1. Das Symbol ist nachvollziehbar.

2. Ich kann dem Symbol vertrauen.

3. Ich kann mich auf das Symbol nicht verlassen. (-)

4. Das Symbol ist zuverlässig.

5. Das Symbol ist präzise.

• Demographics:

Age, Gender, Educational level, Employment status, Privacy and security background, Smart home ownership, AR experience

18. Indices (optional)

For self-efficacy, perceived knowledge, security attitude, symbol trust, and systems trust we will compute mean scale responses. For tested knowledge we will compute the sum of correct responses (each fully correct answer will be coded as one point).

**Analysis Plan**

19. The pretest sensitization hypothesis will be tested with a robust Bayesian estimation for comparing two groups. We make the following assumptions: for data, t distribution; for μ, normal; for σ, uniform; for ν, exponential(1/29) + 1, with the constraint that nu >= 1; ROPE (delta) +-0.42). The other three hypotheses (additive and restrictive self-efficacy effects as well as effect of trust on self-efficacy) will be tested with a (robust) regression model. Post self-efficacy scores are compared across all five intervention groups while the pre-measurement of self-efficacy is controlled for. The intervention group variable will be manually coded as the contrasts of interest (C and B > A; C > B; D > A). The pre-measurement variable will be centered. The model will be formalized as follows: post ~ group + pre. The precise code is attached to this registration.

20. Transformations (optional)

There are some inverse items, which will be re-coded. Please see the “(-)” indication in section 17. Measured variables. Multiple choice answers from the tested knowledge variable are re-coded with 1 for fully correct answer and 0 for partly/completely incorrect answer. The categorical predictor in the regression (group) is coded as a contrasts matrix as follows (the inverse matrix is used as group contrasts):

matrix(c(1/4, 1/4, 1/4, 1/4,

-1, 0.5, 0.5, 0, # additive self-efficacy effect (B and C > A)

0, -1, 1, 0, # restricted self-efficacy effect (C > B)

-1, 0, 0, 1), ncol = 4). # effect of trust on self-efficacy (D > A)

The metric predictor in the regression (pre) is centered.

21. Inference criteria (optional)

For the described Bayesian analysis we will use a ROPE for the posterior distribution on the effect size of delta = +-0.42. This was inferred by the precision analysis (attached to this registration). For the regression analysis we will report the standard p < .05 criteria and confidence intervals for the bias corrected and accelerated coefficients as decision criteria.

22. Data exclusion (optional)

Participants will be excluded from all analysis if (a) they failed one or more attention check items; (b) the intervention could not be completed; (c) they skipped all privacy tasks. Participants will be excluded from the respective analysis if data is missing (e.g., not finished participation, users closed the app or the app froze). Outliers will be analyzed, reported, and included in a robust estimation.

23. Missing data (optional)

Participants will be excluded from the respective analysis if data is missing (e.g., not finished participation). Otherwise in the case of self-reporting, no missingness can occur because the questionnaire is set to force a response.

24. Exploratory analysis (optional)

We also expect interesting results regarding knowledge, behavioral learning, and trust as well as potential intervention differential effects. We will check individual-level data.

**Other**

25. Other (Optional)

Related projects:

Within this project there are two degree theses planned with separate pre-registrations. Those theses focus on different research questions while using the same data.

References:

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215. <https://doi.org/10.1037/0033-295X.84.2.191>

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory. Prentice-Hall series in social learning theory*. Prentice-Hall.

Beggiato, M. (2015). *Changes in motivational and higher level cognitive processes when interacting with in-vehicle automation*. (Doctoral dissertation). Retrieved from http://nbn-resolving.de/urn:nbn:de:bsz:ch1-qucosa-167333

Borgert, N., Reithmaier, O. D., Jansen, L., Hillemann, L., Hussey, I., & Elson, M. (2023). Home Is Where the Smart Is: Development and Validation of the Cybersecurity Self-Efficacy in Smart Homes (CySESH) Scale. In A. Schmidt, K. Väänänen, T. Goyal, P. O. Kristensson, A. Peters, S. Mueller, J. R. Williamson, & M. L. Wilson (Eds.), *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-15). ACM. https://doi.org/10.1145/3544548.3580860

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What We Think We Know About Cybersecurity An Investigation of the Relationship between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context. *Behaviour & Information Technology, 41*(8), 1796-1808. <https://doi.org/10.1080/0144929X.2021.1905066>

Deci, E. L., & Ryan, R. M. (1985). *Intrinsic Motivation and Self-Determination in Human Behavior*. Springer US. https://doi.org/10.1007/978-1-4899-2271-7

European Union (Ed.). (2020). Special Eurobarometer 499: Europeans’ attitudes towards cyber security. https://doi.org/10.2837/672023

Faklaris, C., Dabbish, L., & Hong, J. I. (2019). A Self-Report Measure of End-User Security Attitudes (SA-6). In USENIX Association, *Proceedings of the Fifteenth Symposium on Usable Privacy and Security (SOUPS) 2019.* Symposium conducted at the meeting of USENIX Association, Santa Clara, CA, USA.

Franke, T., Trantow, M., Günther, M., Krems, J. F., Zott, V., & Keinath, A. (2015). Advancing electric vehicle range displays for enhanced user experience: the relevance of trust and adaptability. In *Proceedings of the 7th international conference on automotive user interfaces and interactive vehicular applications* (pp. 249-256).

Jian, J.-Y., Bisantz, A. M., & Drury, C. G. (2000). Foundations for an Empirically Determined Scale of Trust in Automated Systems. *International Journal of Cognitive Ergonomics, 4*(1), 53-71. <https://doi.org/10.1207/S15327566IJCE0401_04>

Trommler, D., Attig, C., & Franke, T. (2018). Trust in activity tracker measurement and its link to user acceptance. In Gesellschaft für Informatik e.V., *Mensch und Computer 2018*, Dresden, Germany.