TECHNISCHE UNIVERSITÄT CHEMNITZ

Faculty of Behavioural and Social Sciences
Institute of Psychology
Professorship of Cognitive Psychology & Human Factors

The Influence of an App's Risk on Trust, Distrust and Intention to Use

Halama, J.[1], Döbelt, S. & Bocklisch, F.

[1] Wilhelm-Raabe-Str. 43, 09120 Chemnitz; josephine.halama@psychologie.tu-chemnitz.de

Background

Users usually did not understand permissions of mobile apps (Kelley et al., 2012; Felt et al., 2012). Therefore, it is difficult to decide **whether to trust a certain app or not and to make informed privacy decisions about using an app.**

Trust in an app is important for users, to form the **intention to use** it (Kelley et al., 2012). It can be defined as a willingness to be vulnerable to the trustee based on the expectation that the trustee will perform in a positive manner (Mayer et al., 1995). Probably related but distinct from trust is the construct of **distrust** (e.g., Lewicki et al., 1998). It occurs *"when the distruster expects that the other party will act in a negative manner" and not* as desired (Moody, 2010, p. 16).

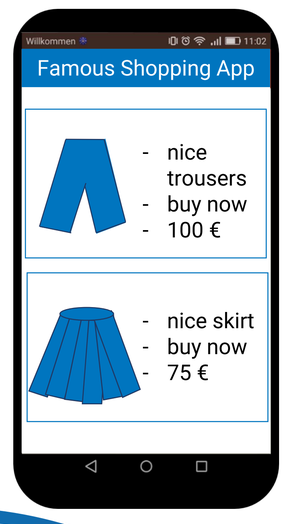
While trust was studied intensively, **distrust** was rather **neglected** (e.g. Lankton et al., 2015). Therefore, the research question arises **whether trust and distrust are different constructs** or not.

Hypotheses (H) derived from literature:
- **H1: Distrust** and **trust** are **distinct** constructs**.**
- **H2: Transparency about the risk** of a high-risky app leads to
  - **lowered trust** (H2a)
  - **increased distrust** (H2b)
  - **lowered intention to use** the app (H2c)

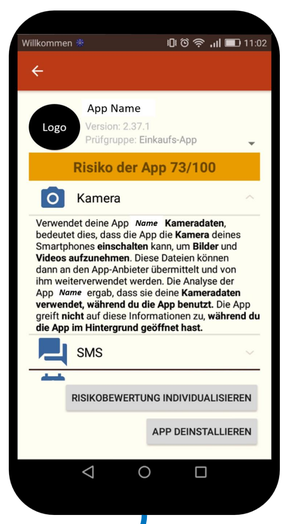
Method

- context: privacy symposium
- *N* = 16 pedagogues (10 female, 5 male, one without specification); age: *M* = 39.27 years (*SD* = 11.97)

video: shopping app → pre-evaluation shopping app → video: risk analysis of shopping app

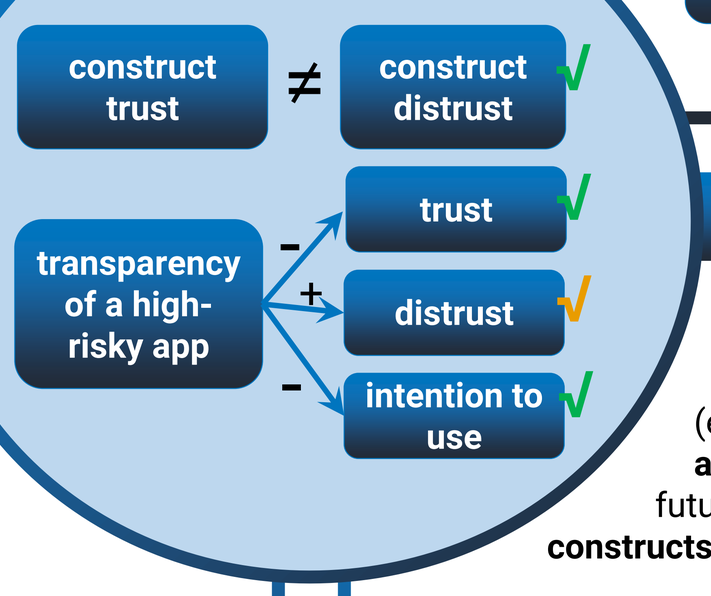


questionnaires
- **trust**: 9 items; scales: integrity, competence, benevolence (Lankton et al., 2015)
- **distrust**: 9 items, deceit, incompetence, malevolence (McKnight & Choudhury, 2006; omitting items 7 and 11; scale labels from Moody, 2010)
- **intention to use** (1 item; likelihood to use the shopping app, from 1 to 10)



post-evaluation shopping app

Summary

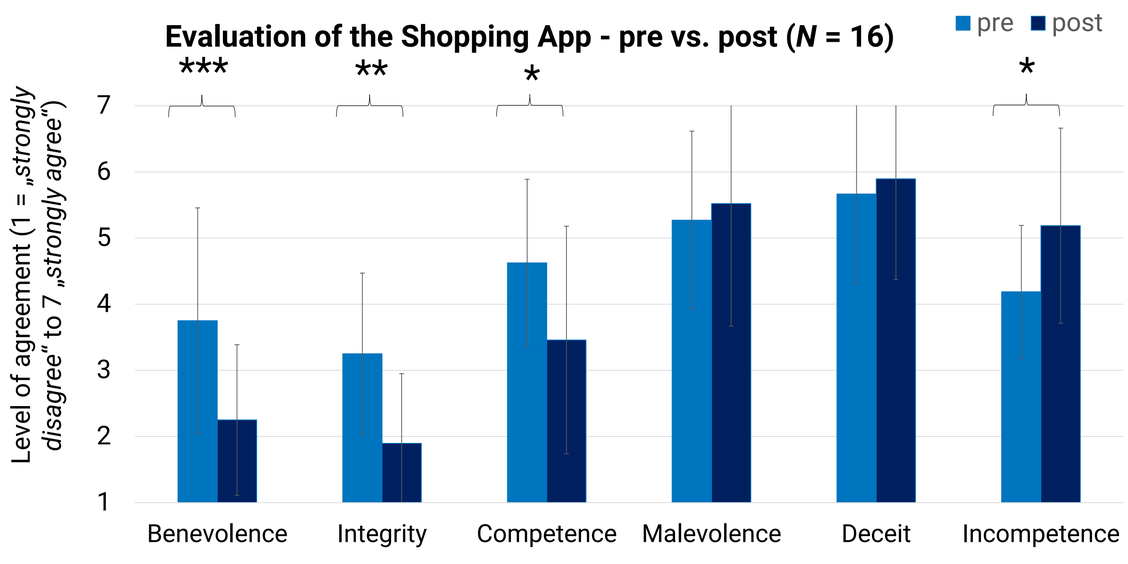


Results

H1: large effect sizes and significant differences between corresponding trust and distrust scales
→ H1 supported
- benevolence vs. malevolence: z = -2.33, p = .02, d = 1.42
- integrity vs. deceit: z = -2.28, p = .02, d = 1.39
- competence vs. malevolence: z = -2.00, p = .05, d = 1.15

(to test H1 means of the trust/distrust scales were calculated, values for distrust inverted)

H2: medium to large effect sizes, almost always significant differences between pre and post values
→ H2 supported
- H2a (trust): significant and large effects for all comparisons
- H2b (distrust): significant and large effect for incompetence, non-significant but medium effects for malevolence and deceit
- H2c (intention to use): pre: *M* = 3.75, *SD* = 3.53; post: *M* = 2.06, *SD* = 2.74, *d* = 2.74; significant and large effect



Discussion

All comparisons of the corresponding trust and distrust scales lead to significant differences and large effect sizes. In line with related work (e.g., Lewicki et al., 1998), **distinctiveness of trust and distrust was confirmed** (**H1**). Therefore, future research on apps should **include both constructs.**

The data also confirmed H2. However, the pre-post-differences between the distrust scales malevolence and deceit were not significant. This lack of significance is probably caused by the small sample size.

Surprisingly, the differences between the **pre-post** comparisons (H2) on **trust** were **larger** than the differences on **distrust**. One might assume that transparency of a high-risky app has a larger impact on distrust. Considering the descriptive data of the two scales, the values were very large even before the intervention. These values might result from the purpose of the symposium and participant's expectations.

But even with this sample, **transparency about the risk of an app can lead to a more appropriate assessment and an informed decision about the usage.**

ALLGEMEINE & PSYCHOLOGIE & HUMAN FACTORS

References

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In L. F. Cranor (Ed.), *Proceedings of the Eighth Symposium on Usable Privacy and Security,* 3. doi:10.1145/2335356.2335360

Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A Conundrum of Permissions: Installing Applications on an Android Smartphone. In J. Blyth, S. Dietrich, & L. J. Camp (Eds.), *Financial Cryptography and Data Security,*. 68-79. Berlin, Heidelberg: Springer. doi: 10.1007/978-3-642-34638-5_6

Lankton, N. K., McKnight, D. H., & Trip, J. (2015). Technology, Humanness and Trust: Rethinking Trust in Technology. *Journal of the Association for Information Systems, 16* (10), 880 -918.

Lewicki, R., McAllister, D. J., & Blies, R. J. (1998). The Academy of Management Review, 23 (3), 438-458. doi: 10.2307/259288

Mayer, R. C., Davis, J. H., & Schoorman, F. D., 1995. An Integrative Model of Organizational Trust, Academy of Management Review, 20(3), pp. 709-734.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334-359.

Moody, G. D. (2010). *The Hybrid Model of Trust and Distrust: Extending the Nomological Network* (Dissertation), University of Pittsburgh, Pittsburgh.