# Social Engineering

Geschichte, Wirkung, Wissenschaft

Alles, was ihr immer über Social Engineering wissen wolltet, aber nie die Zeit hattet, zu erfragen.

*- k4tana -*

# New talk who dis?

- IRL Oliver D. Reithmaier
- Psychologe, Social Engineer
- Wiss.MA & Doktorand
  @ Fachgebiet Usable Security & Privacy,
  Leibniz-Universität Hannover
- Mag: Nerd-Kram, Social Engineering, Forschung, Geschichte, Daten & Privacy.

# Story time!

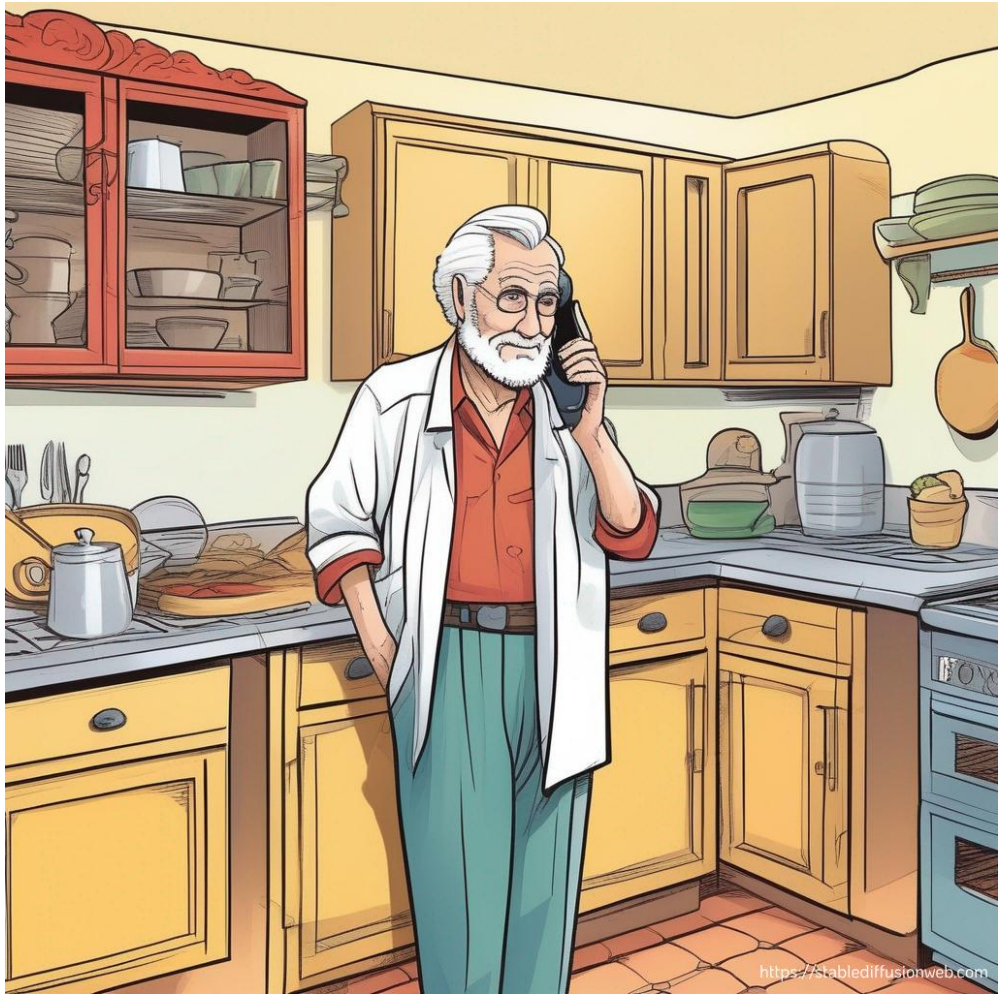



Bild: stablediffusionweb.com (ML generiert)

# Definition

**Praktiker:**

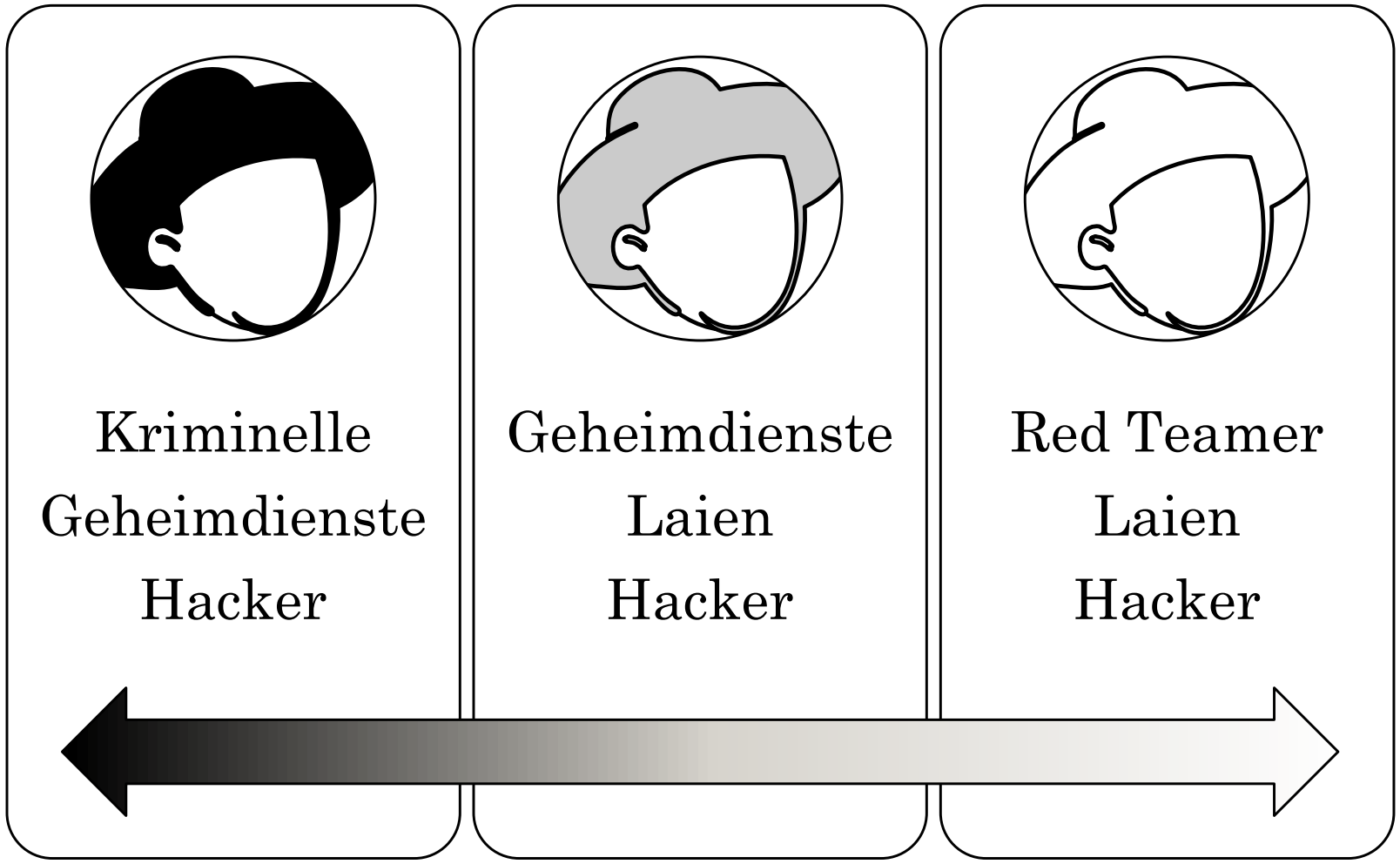
„Social Engineering is **any act that influences a person** to take an action that may or may not be in their best interest“ [Hadnagy, 2018].

**Wissenschaftler:**

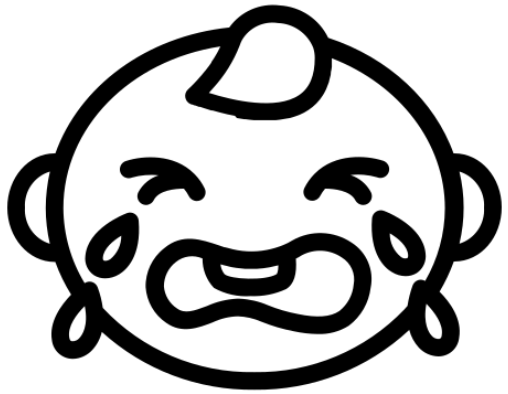
“Social Engineering (SE) is focused on the **exploitation of a human** in order to gain unauthorised access to information” [Mouton et al., 2014].


Bild: stablediffusionweb.com (ML generiert)

# Akteure


Kriminelle
Geheimdienste
Hacker
Geheimdienste
Laien
Hacker
Red Teamer
Laien
Hacker

# Ihr alle seid/wart mal Social Engineer!



# Geschichte

Es ist eine lange!

# Social Engineering im Laufe der Zeit

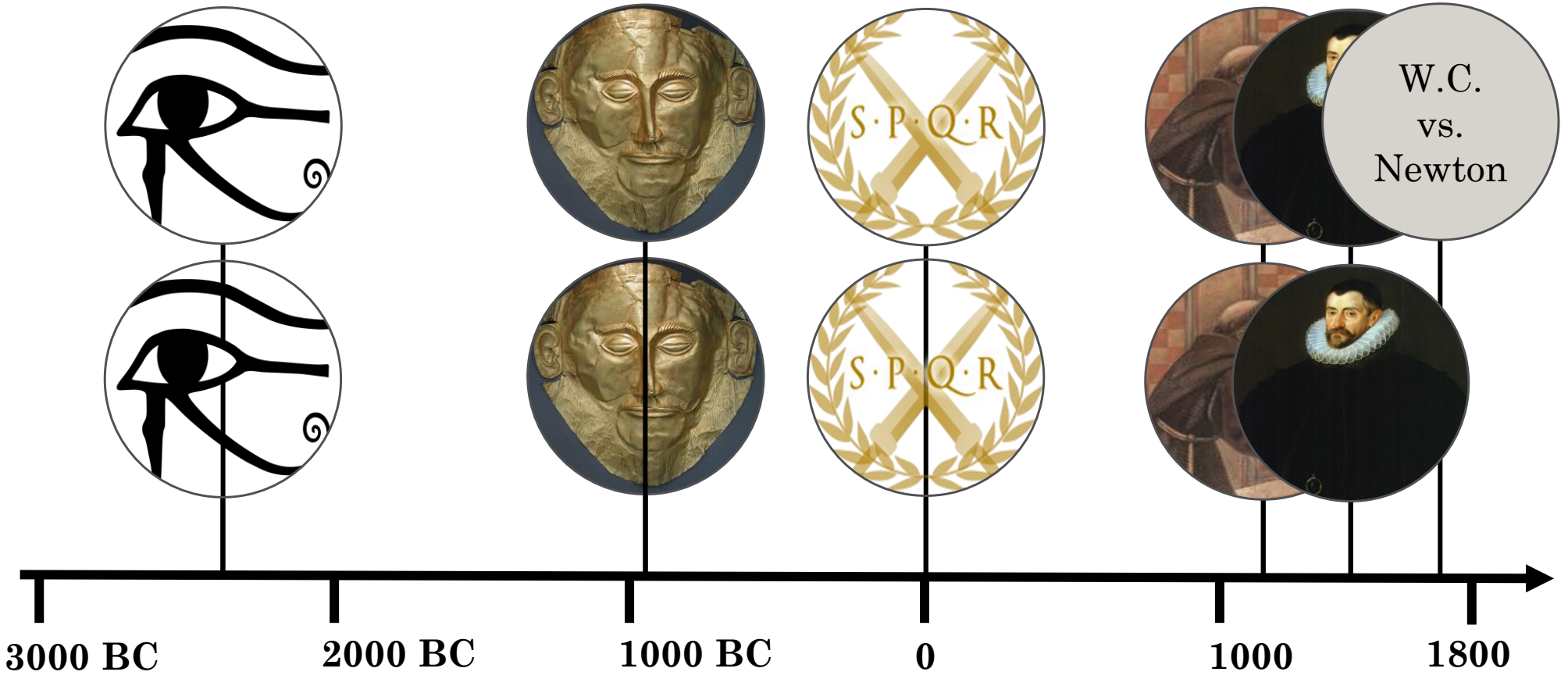
Erster bekannter Social Engineer war ein Black Hat!



Bilder: Tima Miroshnichenko/Pexels,
stablediffusionweb.com (ML generiert)

# Social Engineering im Laufe der Zeit

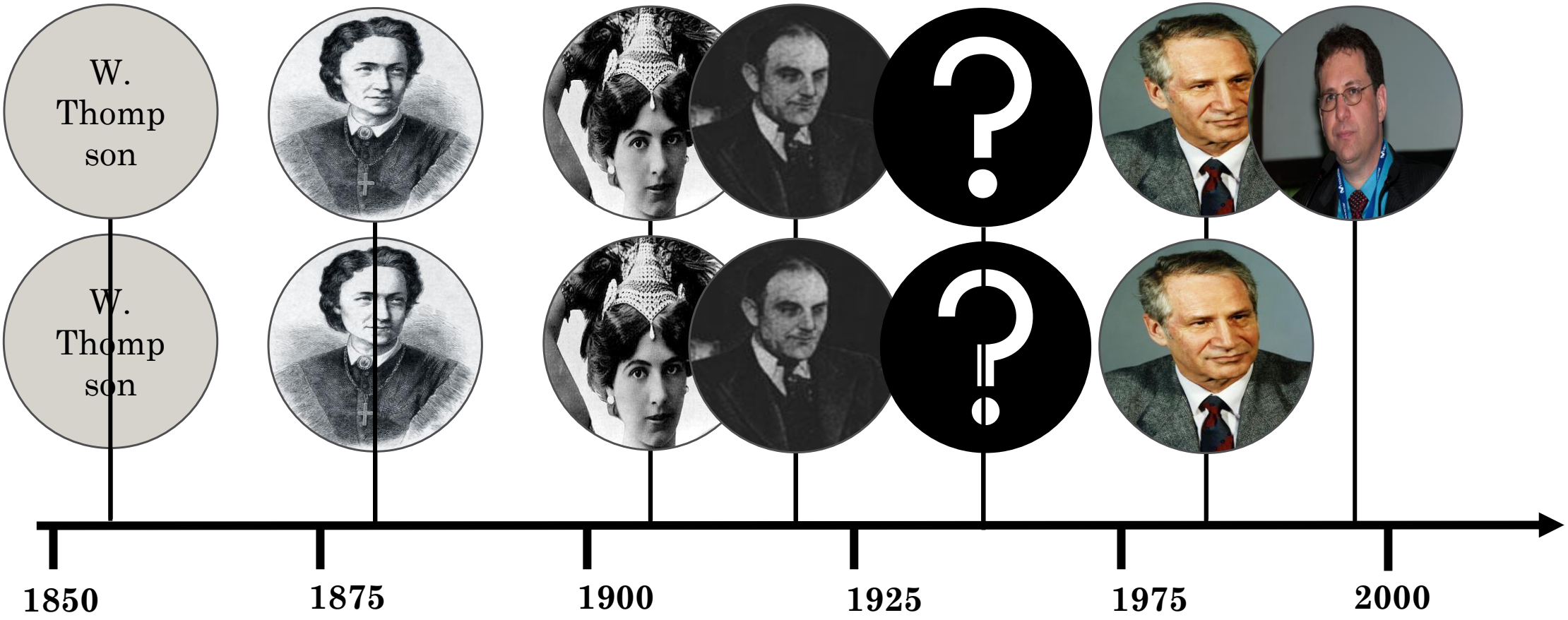
## Highlights aus 5000 Jahren Menschheitsgeschichte




Alle Bilder: Wikipedia.org, Creative Commons

# Social Engineering im Laufe der Zeit

Highlights aus 5000 Jahren Menschheitsgeschichte

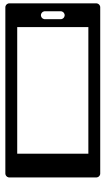



Alle Bilder: Wikipedia.org, Creative Commons

# Social Engineering heute

**Das Meiste: Phishing**

„Phishing *electronically* **deceives a user to conform to some action**, subsequently, divulging sensitive Information.“
(Jansson & Solms, 2013)



# Social Engineering: Heute

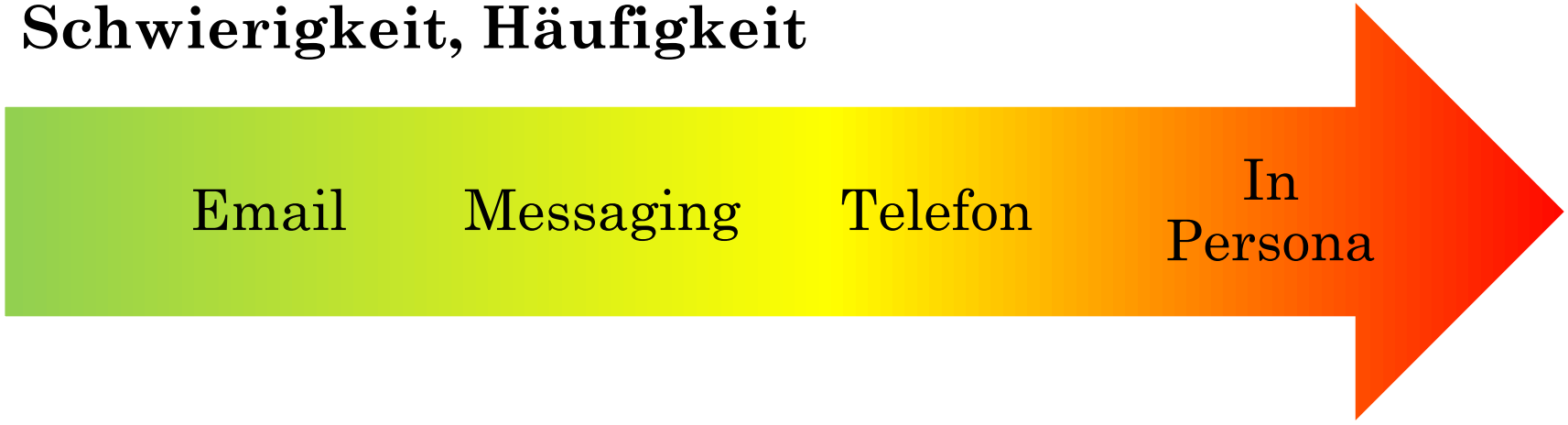
**Phishing**

- Email
- Telefon
- Messaging
- Deepfakes (Video/Audio)

**In Persona**

- Industriespionage
- Geheimdienstliche Operationen
- Verdeckte Ermittlung
- Trickdiebstahl

**Schwierigkeit, Häufigkeit**



# Wirkung

Psychologie von SE

# Vier-Ohren-Modell

- Friedemann Schulz von Thun, 1981
- Beschreibt Missverständnis-Quellen in der Kommunikation.
- Missverständnisse sind immer Sender/Empfänger Konflikte hinsichtlich der Ebene, die verstanden wird.

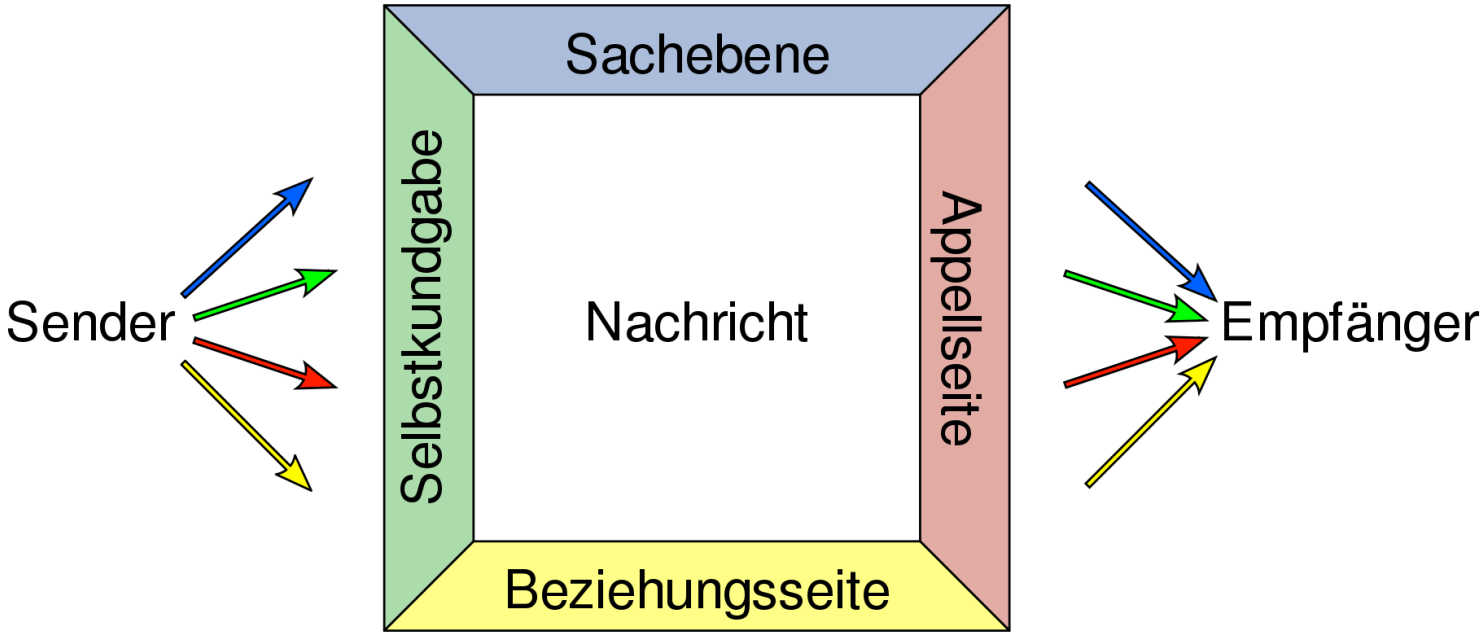
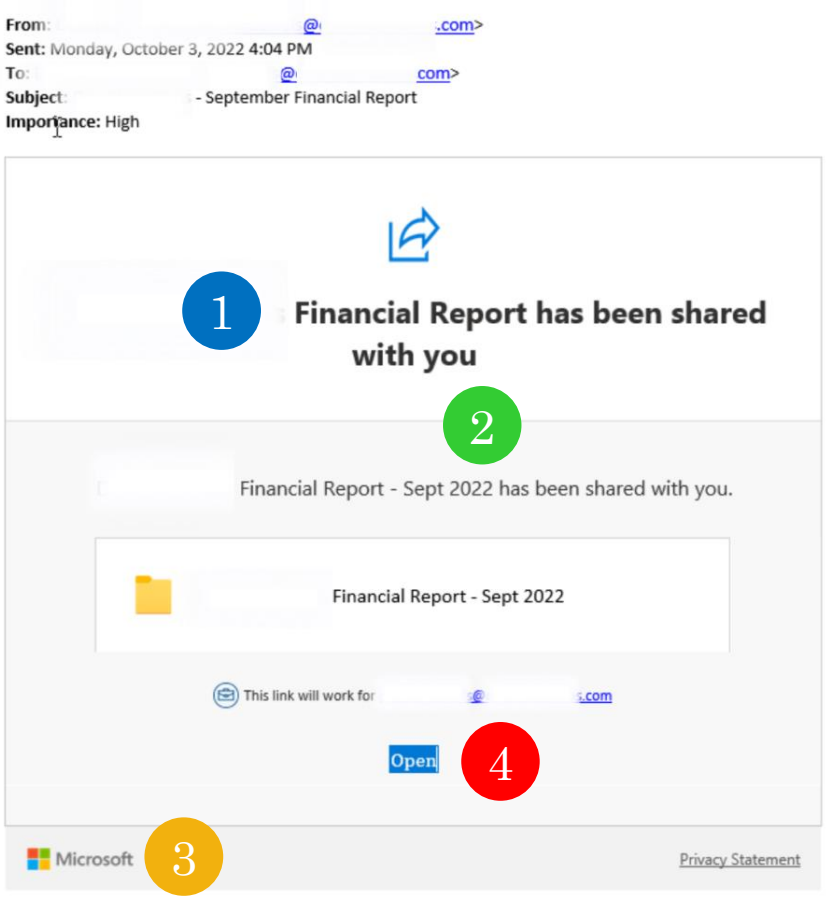



Bild: https://de.wikipedia.org/wiki/Vier-Seiten-Modell#/media/Datei:Vier-Seiten-Modell_de_2.svg

# Beispiel: Phishing Email

SENG konstruiert die Nachricht so, wie sie in den „Ohren“ *ankommen soll.*

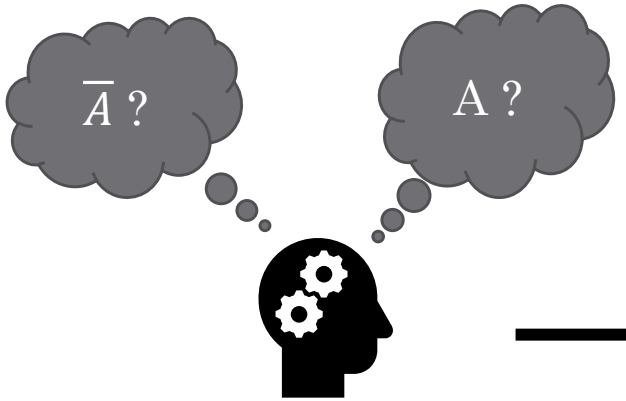



| | | |
|---|---|---|
| 1 | **Sachebene** | Hier ist eine neue Datei für dich! |
| 2 | **Selbstoffenbarung** | I bims, 1 Bot. |
| 3 | **Beziehungsebene** | Ich bin ein freundlich, wir kennen uns 😉 |
| 4 | **Appell** | Log dich ein und guck nach! 🧐 |

Bild: https://technologyassociates.net/general/how-to-spot-a-popular-microsoft-onedrive-email-phishing-scam/

# Kognitive Dissonanz

- Leon Festinger (1962)
- Ereignisse A und $\overline{A}$ sind erstrebenswert, stehen einander aber im Weg.




A | $\overline{A}$

Frymier & Nadler, 2007
Festinger & Carlsmith, 1959

Negative Konsequenzen?
Wahlfreiheit?
Internale Rechtfertigung?

**SE:**

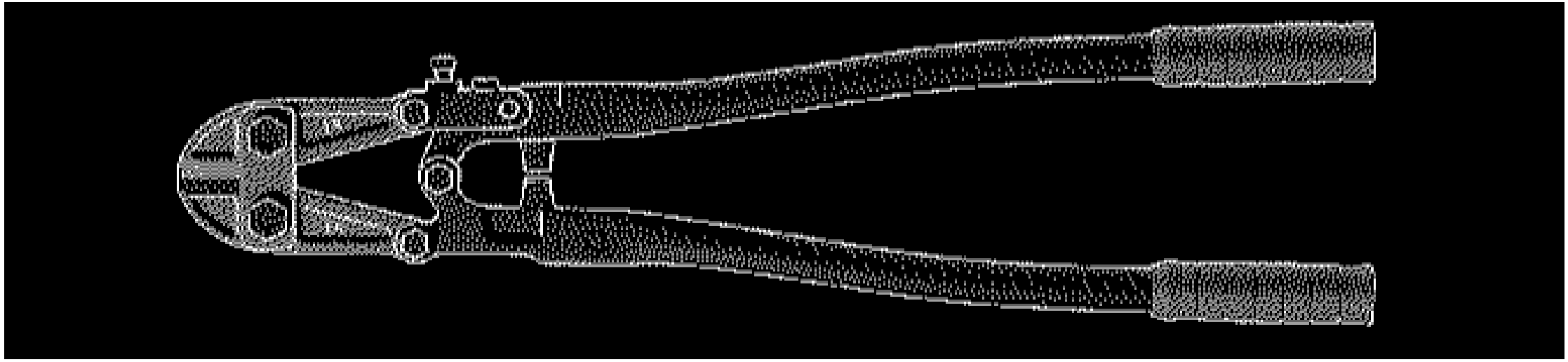
- *Künstliches* B erzeugen, wenn nur A existiert.
- *Rahmenbedingungen anpassen*
- *Einstellung verändern* etc., sodass A verliert.

# Beispiel: Kognitive Dissonanz

Bild: https://www.golem.de/news/cyberbunker-prozess-die-darknet-schaltzentrale-ueber-den-weinbergen-2010-151444.html

# Beispiel: Kognitive Dissonanz

- Aushebung des Cyberbunkers war nur durch Social Engineering möglich.
- Zentrale Dissonanz:
  Mit allen Essen gehen/feiern **vs.** „Mind. einer muss den Bunker bewachen“
- Rahmenbedingungen angepasst: Gefahr heruntergespielt.
- Einstellung abgeschwächt: „Einmal ist keinmal“, „so jung kommer nimmer zam“ etc.



Bilder: Wikipedia, CCC.

# Elaboration-Likelihood-Model

- Richard E. Petty & John Cacioppo 1986

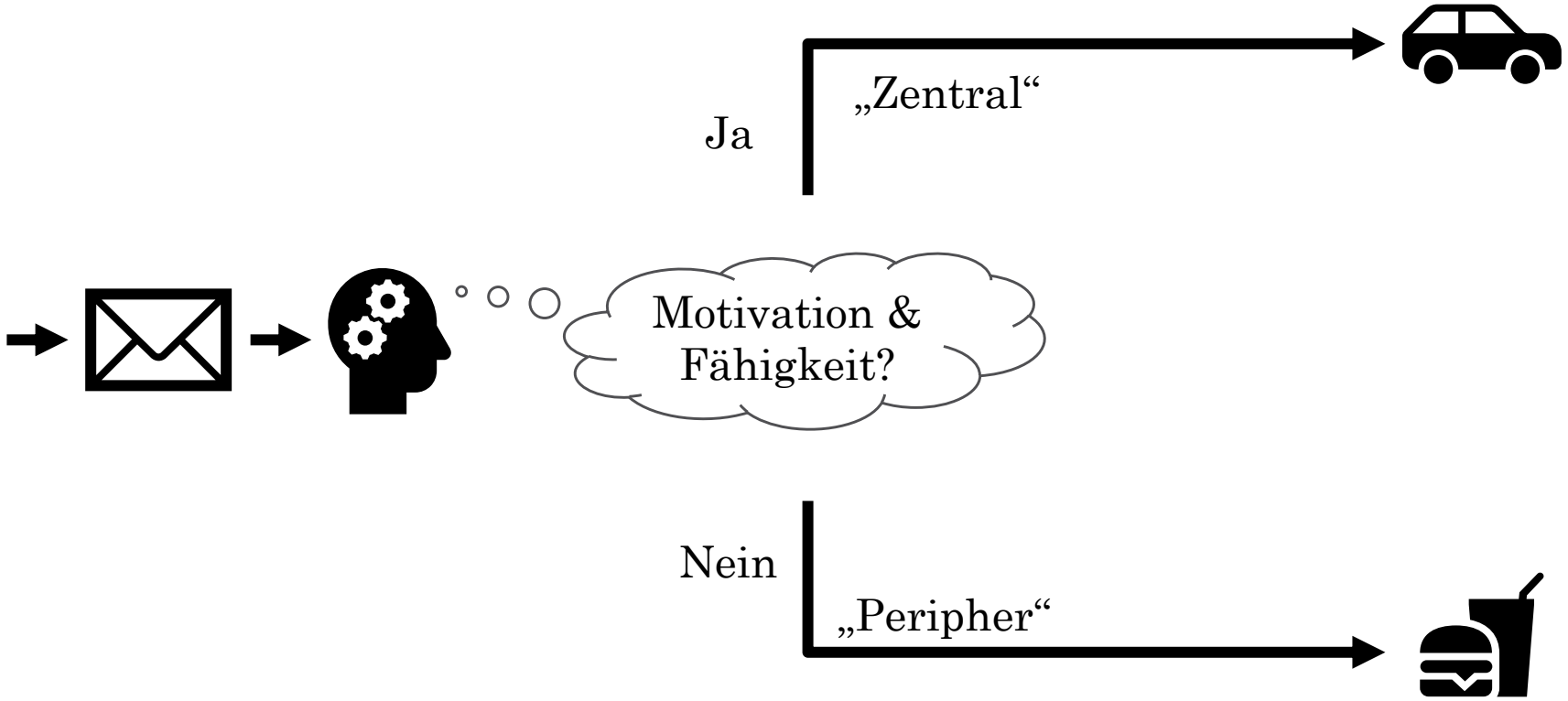
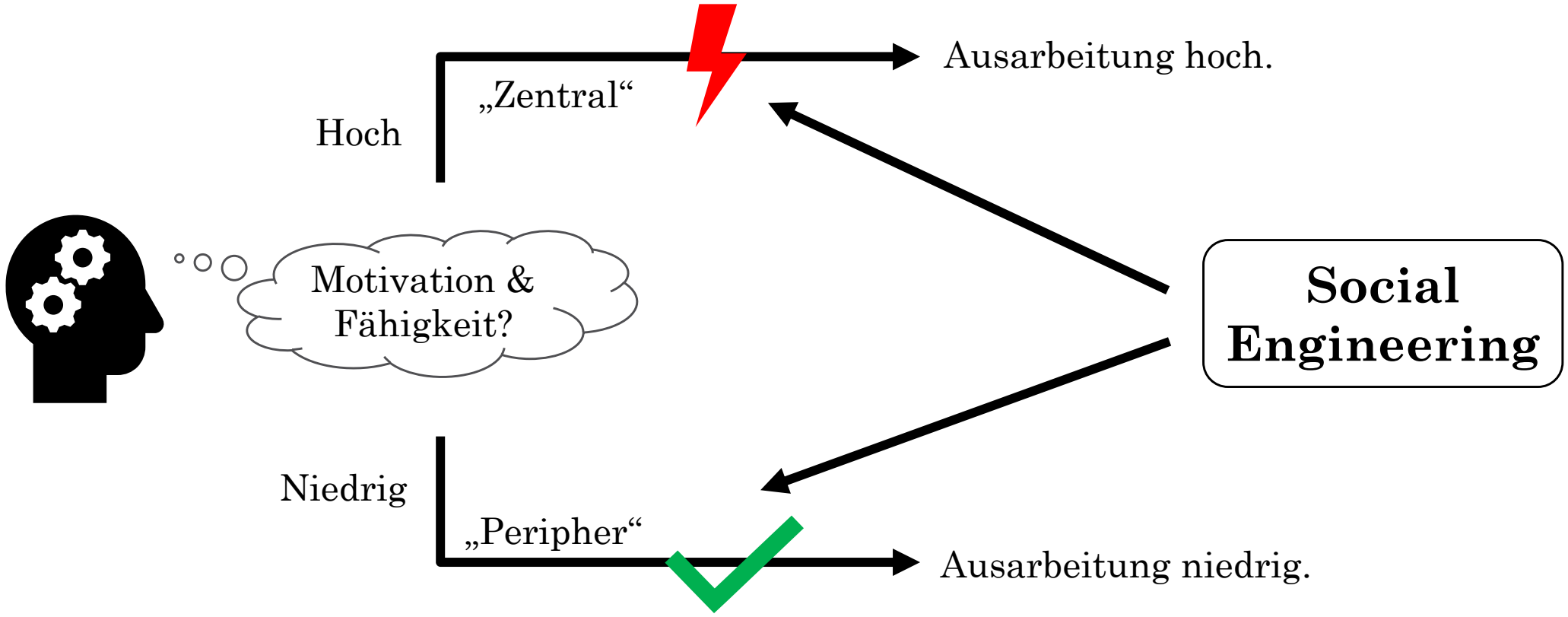


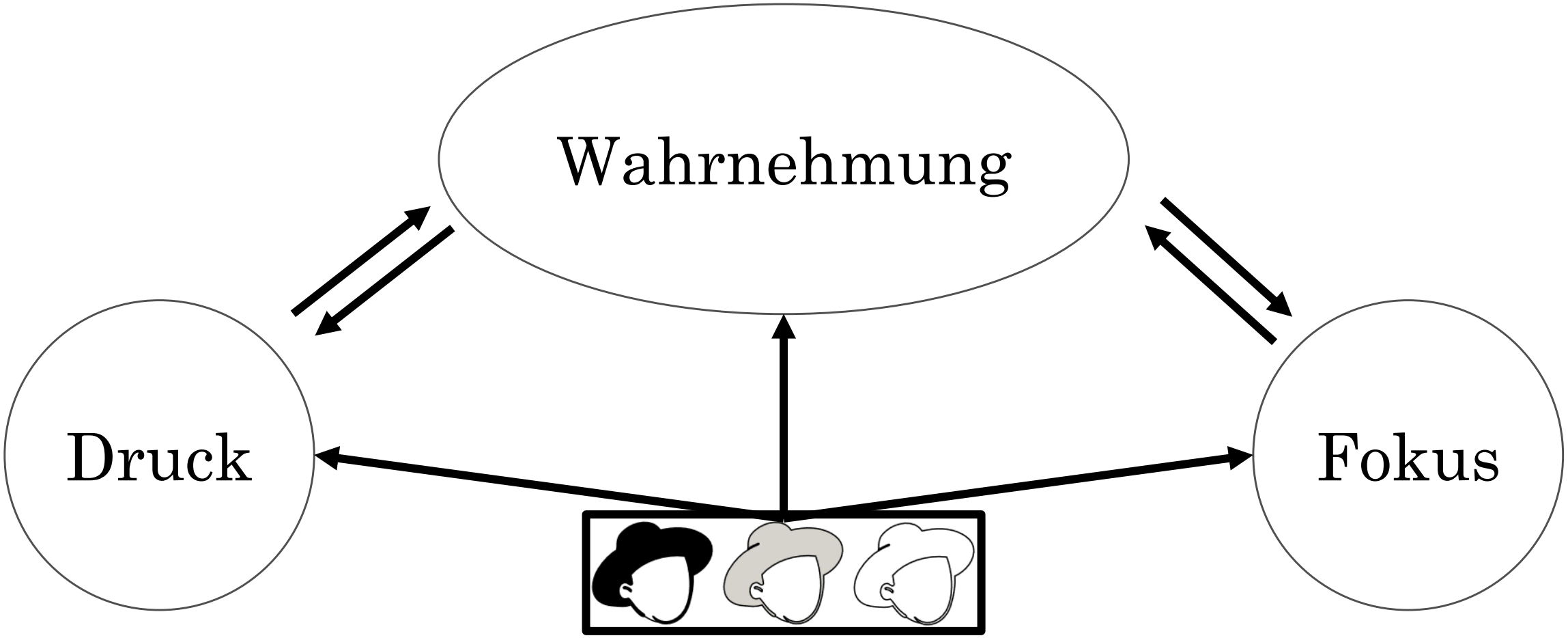

Bild: Antonio Friedemann / Pexels

# Elaboration-Likelihood-Model (2)

- Richard E. Petty & John Cacioppo, 1986



# Rahmenbedingungen



# Wie oder was angreifen?

Bias, Prinzipien & Techniken

# Warum wirkt Social Engineering?

**TLDR: Wir sind alle Menschen. Menschen haben immer (u.a) folgende Charakteristika**

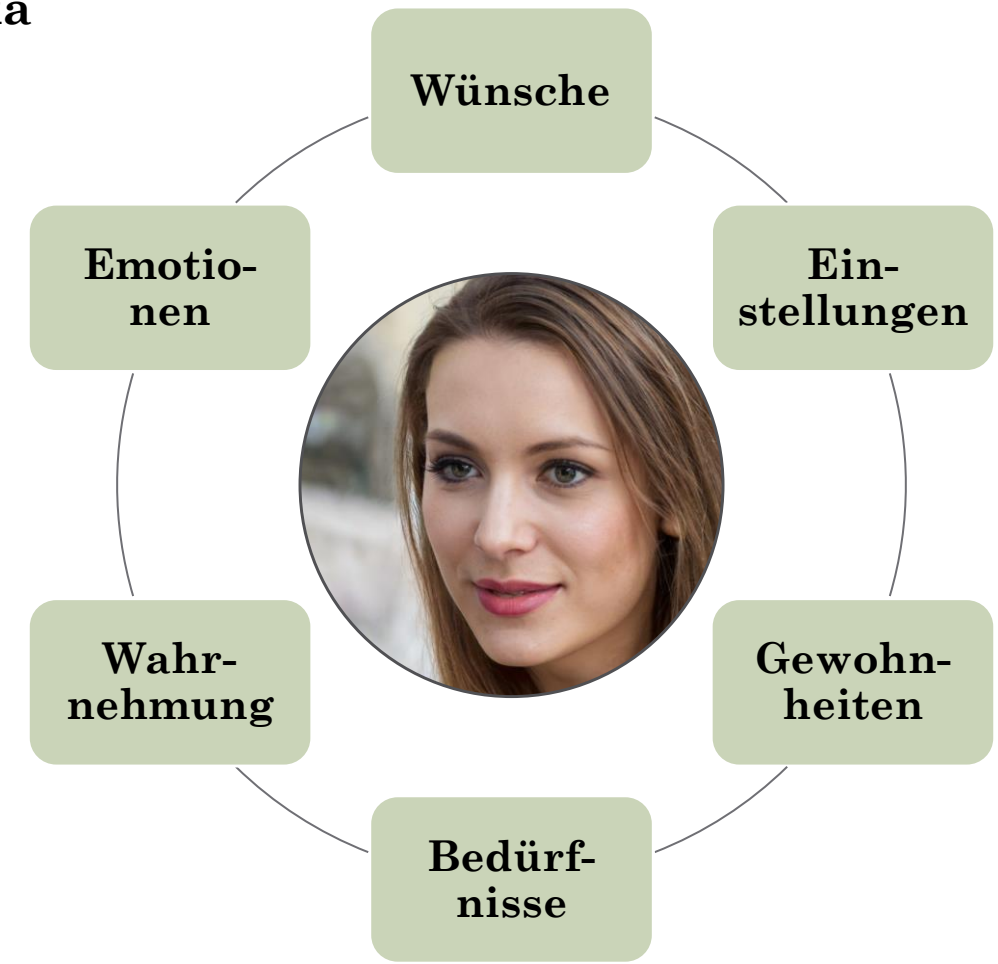
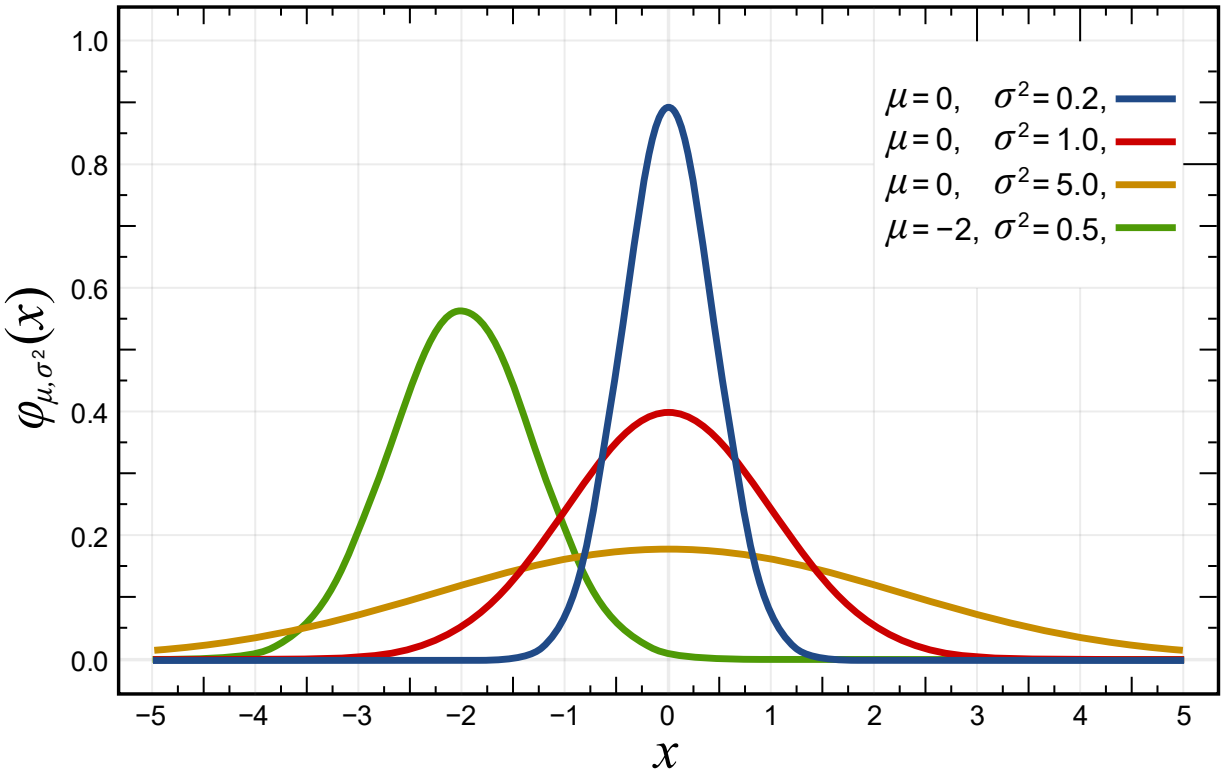



Bild: thispersondoesnotexist.com

# Bei wem wirkt Social Engineering?

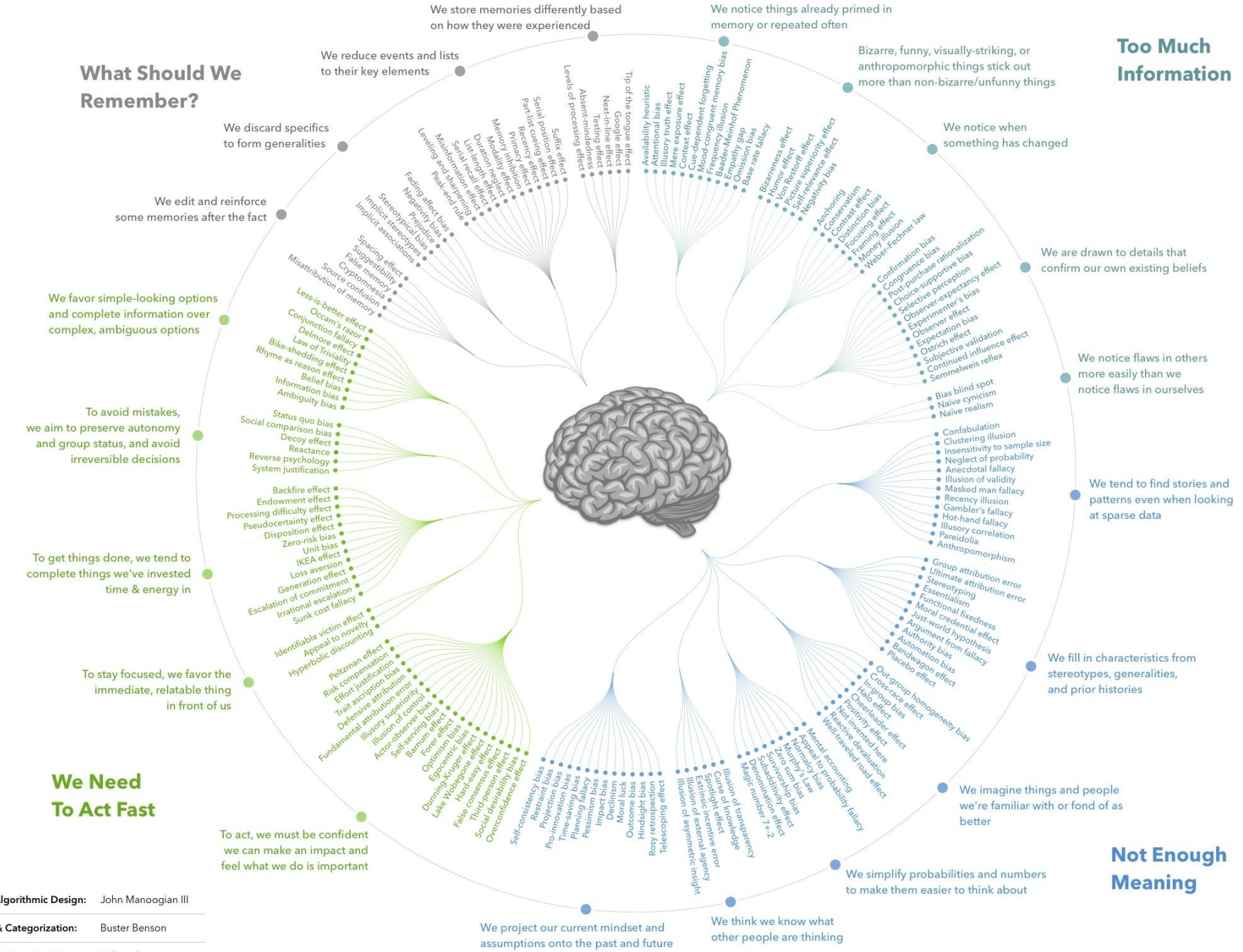
- **Bei allen sozialen Lebewesen**
- **Variable Effekte:** Je nach ausgenutztem Mechanismus und Ziel.
- **SE ist Glücksspiel.** Wer gut mit Risiko und Wahrscheinlichkeit umgehen kann, ist tendenziell besser darin.



# Kognitive Verzerrungen (Bias)

- **Generelle Tendenzen**, Denkmuster
- Beeinflussen **Erleben (Wahrnehmung, Denken) und Verhalten**.
- Erleben und Verhalten werden **in eine bestimmte Richtung „verzerrt“**

# COGNITIVE BIAS CODEX




| | |
|---|---|
| **Visual & Algorithmic Design:** | John Manoogian III |
| **Concept & Categorization:** | Buster Benson |
| **List of 188 Cognitive Biases:** | Wikipedia |

designhacks.co

# Beispiele: Kognitive Verzerrungen (Bias)

Confirmation Bias (Wason, 1960)

**Bias Blind Spot** (Pronin & Lin, 2002)


IKEA Effekt (Norton et al., 2012)

Framing Effect (Tversky & Kahnemann, 1981)

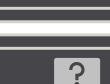
# Principles of Social Influence

- Robert B. Cialdini (1984), ursprünglich aus der Marketingpsychologie.


Reziprozität


Autorität


Knappheit/Mangel


(Internale) Verbindlichkeit & (externale) Konsistenz

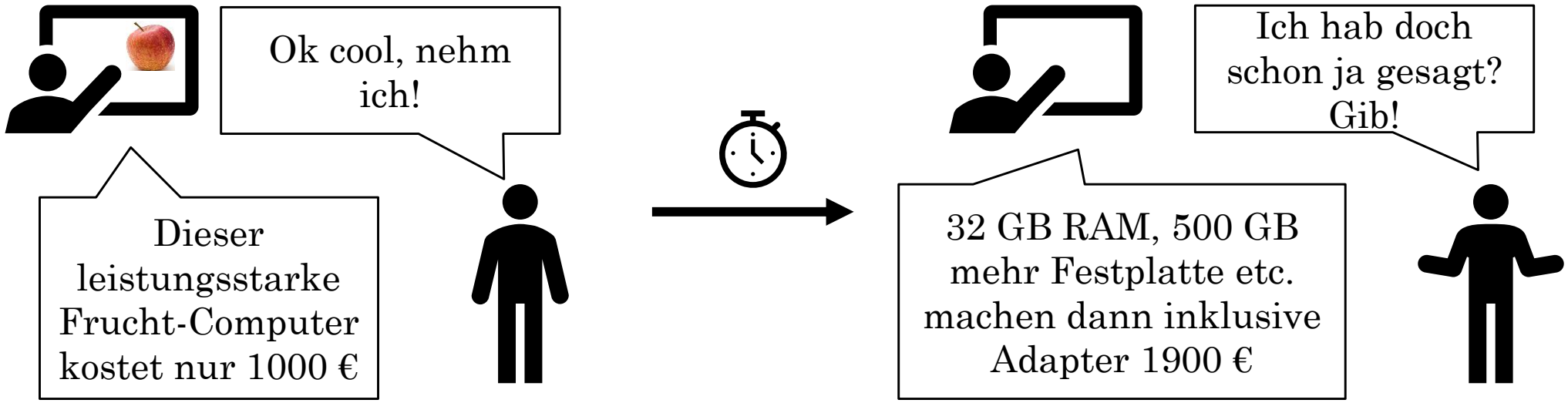

Sozialer Beweis


Sympathie

# Technik: Beispiel

**Lowballing**

- ~~Scam~~ Verkaufs-Taktik. Nutzt Verbindlichkeit und Konsistenzstreben aus.
- „Bild verkaufen, dann jeden Pinselstrich einzeln berechnen.“
- Erste wissenschaftliche Beschreibung: Cialdini, Cacioppo, Bassett, & Miller, 1979.



# Zusammenfassung

- SE wirkt im Kopf
- Alles innere ist angreifbar, weil wir Menschen sind.
- Das geht auch nicht weg. Und selbst wenn du glaubst, dass du es weg hast, unterliegst du schon wieder einem Bias.

„Aber k4tana, was ist mit dem tollen Wissen über unbewusstes Verhalten, das mir der freundliche FBI-Typ beigebracht hat?“

# Non-verbales Verhalten

*tiefes seufzen*

# Beispiel: Power Posing

- Sollte mehr Selbstsicherheit und messbare (positive) Änderung in Verhalten und Physiologie geben (Carney et al., 2010).
- Katastrophaler wissenschaftlicher Absturz:
  - **Replikationen gescheitert**, keine Effekte auf Verhalten oder Physiologie (Ranehill et al., 2015; Garrison et al., 2016; Deuter et al., 2016; Smith et al., 2017)!
  - **Oft keine Kontrollgruppen** oder schlechte Kontrollkonditionen (slouching) → „Poison-Medicine Problem“
  - **Meta-Analyse**: **Null-Effekte** für Verhalten (Simmons & Simonsohn, 2017)
- Zurückrudern später: Ja ok, keine physiologischen oder Verhaltensmerkmale, aber dafür bestimmt kognitive!!1einself (Cuddy et al., 2018)

Bild: Erik Hersman / Wikimedia

# Reaktion von Praktikern

# Emotionen?







Bilder: Paul Ekman Group, paulekman.com (14.12.2023)

# Übertragung auf Deception Research?

# Täuschende Sicherheit

- Methodologisch **teilweise schlecht gemachte Studien** (Plamper, 2015)
- Teilweise **schwer replizierbar** (Russell & Fernández-Dols, 1997)
- Alterstechnisch **teilweise ohne Diversität** (s. Ekman et al., 1969)
- **Teilweise tautologisches Design**. (s. Ekman et al., 1969)
- FACS (Facial Action coding System) ist umstritten.

# Deception „research“.

- Grundidee: Es gäbe nonverbale Kommunikation, die Deception kennzeichnet. Praktiker: Wer das überwinden kann, ist der ultimative SENG
- Von vielen SENGs hoch gepriesen.
- Teil des Mythos, dass non-verbale Kommunikation in das toolkit jedes SENGs gehört. Weil SENGs ja deception beruflich machen.

**Qualität: oft =**


Quelle: wikipedia.org, Logo nur namensrechtlich geschützt.

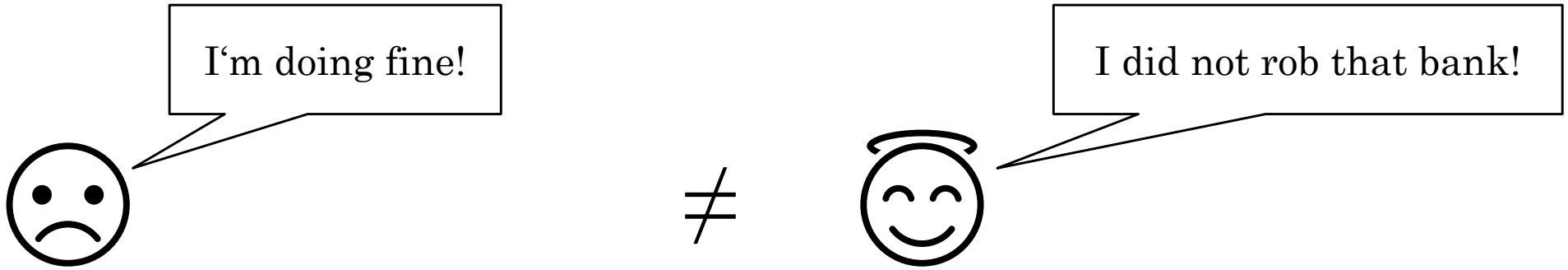
# Post-Faktische Praxis?


**Es ist ein systematisches Problem im Haus!**

# Psychologischer Hintergrund

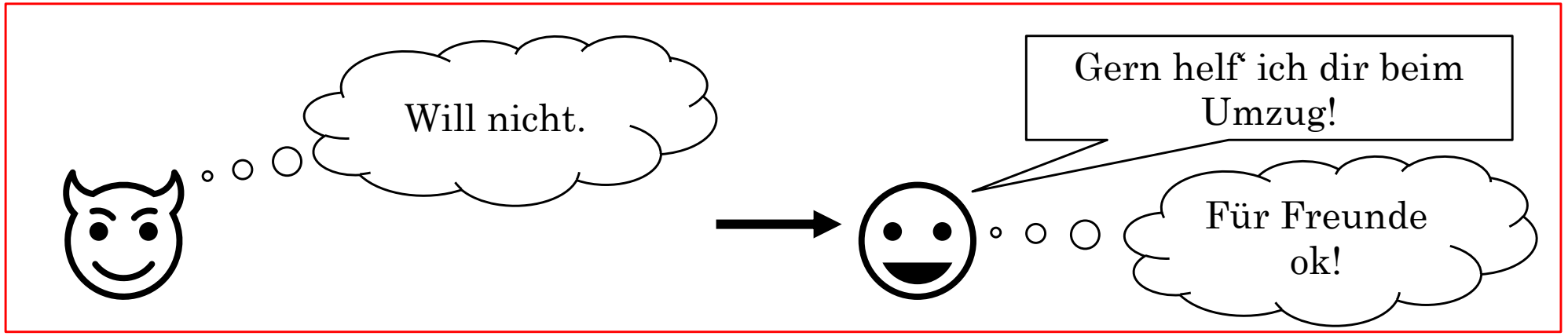
**Grundsätze:**

**1. Unbewusstes und Bewusstes haben oft nichts miteinander zu tun.**




**2. Unbewusstes wird oft bewusst korrigiert.**

Kognitive Dissonanz!



# Psychologischer Hintergrund (2)

**Nebensätze:**

- **Menschliches Verhalten entspringt oft Normen oder Gesetzen.** Die sind nicht immer sinnvoll („maladaptiv“).
- **Menschen sind routineanfällig.** Routinen sind nicht unbedingt rational begründet.
- **Kulturelle Umgebung** bestimmt oft Normen und Gesetze.
- **Menschliches Verhalten ist zum größten Teil gelernt**, d.h. es kann verlernt werden.

# Psychologischer Hintergrund (3)

**Normen**
**Empathie**
**Stereotype**
**Ausdruck**
**Verständnis**
**Wissen**


**Normen**
**Empathie**
**Stereotype**
**Ausdruck**
**Verständnis**
**Wissen**

**Es ist einfach nie garantiert, dass das, was du meinst, auch in der Art und Weise ankommt!**

Bilder: thispersondoesnotexist.com, wikimedia images/Pixabay

# Ist das sinnvoll untersuchbar?

Meiner Meinung nach: nein.
Und selbst wenn ich Unrecht habe, bezweifle ich die Ethik dessen.

Plus: Es scheint sehr irrelevant zu sein.

# Maßnahmen

Was hilft, was nicht?

# Disclaimer

# Was nicht so gut ist.

- **Phishing-Simulationen:** „Board Fodder“, Vertrauensverlust ins Unternehmen, Selbstwirksamkeitsprobleme bei Mitarbeitenden, Hidden Costs (Brunken et al., 2023; Volkamer et al., 2020, Sasse et al., 2023)
- **Zeitdruck** bei der Arbeit (Jones et al., 2019)
- **Schlechte (arbeitspsychologische) Unternehmenskultur** (Solomon & Brown, 2021).
- **Sensitising, Bildung allein** („Schulung“) (Sasse et al., 2023)
- **Schlechter (gelernter) Umgang mit Emails** / digitaler Kommunikation allgemein (Distler, 2023)
- Der übliche Mist („Achten Sie auf Rechtschreibung“/“Grammatik“)

# Was hilft gegen Social Engineering?

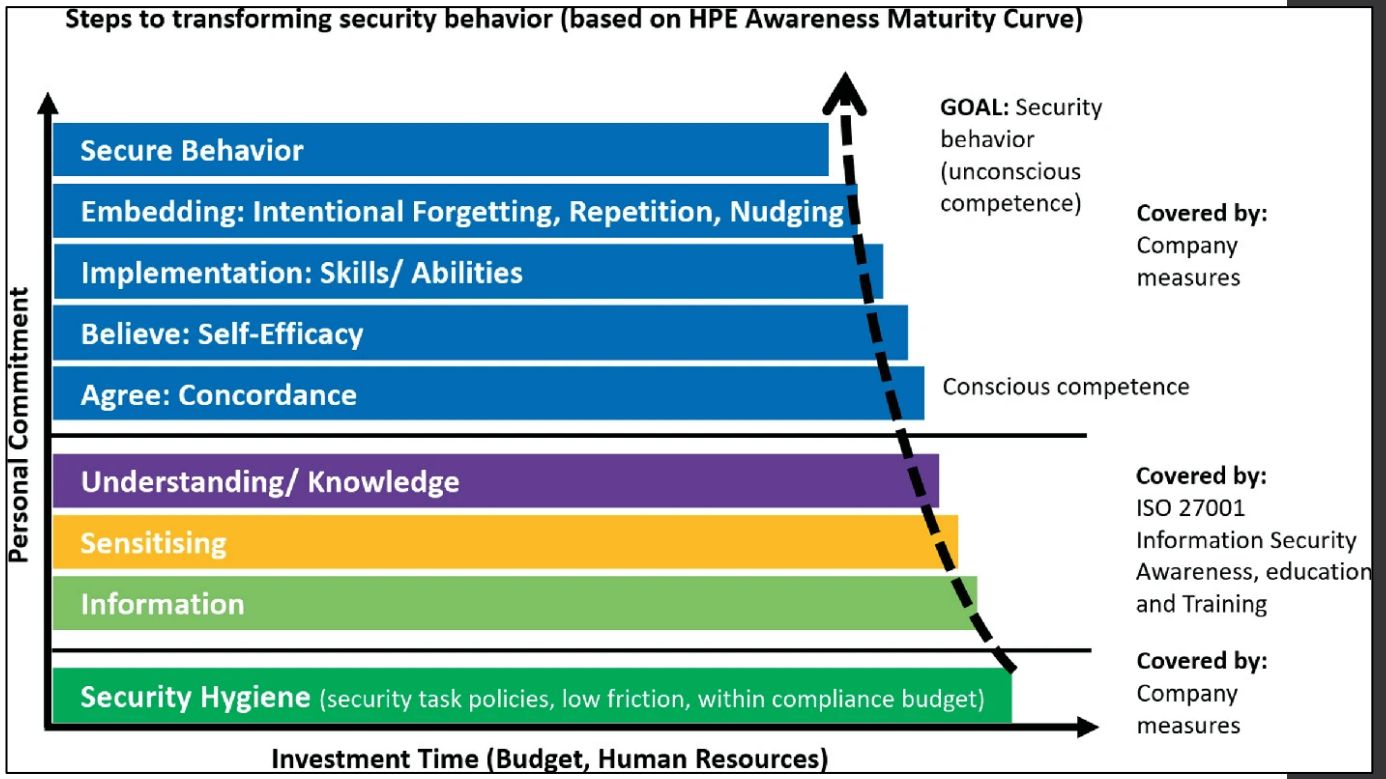
**Für Alle:**

- **Basis = Bildung!** Sich über Phishing und Social Engineering informieren.
- **Auf dem Laufenden bleiben:** Phishing Radar der Verbraucherzentrale im Auge behalten (bspw. auf Mastodon!)
- **Hoch entropische Passwörter verwenden (+PW Manager).**
- Wenn möglich auf **Passkeys** umsteigen.
- **Links überprüfen**; über Suchmaschinen ansteuern, wenn zu Aktion aufgerufen wird („Anmelden“ etc).
- **Zeit nehmen** für Emails und sich nur darauf fokussieren (Distler, 2023).

# Was hilft gegen Social Engineering?

**Für Organisationen vs. Phishing:**

- **Messung** von Wissen und Selbstwirksamkeitserwartung gleichzeitig, sonst verzerrte, zu subjektive Werte (Gründe: Kim et al., 2016; Dang et al., 2020).
- **Einzeltraining**, basierend auf diesen Messwerten (Sutter et al., 2022).
- Sicherheit als Teil der **Organisationskultur** etablieren und eine moderne Organisations-kultur entwickeln (Sasse et al., 2023; Solomon & Brown, 2021).
- **Effektive IT-Security** mit finanziellem Handlungsspielraum schaffen.




Bildquelle: Hielscher et al., 2021

# Ich habe fertig. Gerne Fragen!

**@odr_k4tana@infosec.exchange**
https://infosec.exchange/@odr_k4tana

# Quellen


1. *Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception | IEEE Journals & Magazine | IEEE Xplore*. (n.d.). Retrieved 28 December 2023, from https://ieeexplore.ieee.org/abstract/document/9893815
2. Brunken, L., Buckmann, A., Hielscher, J., & Sasse, M. A. (2023). *{"To} Do This Properly, You Need More {Resources"}: The Hidden Costs of Introducing Simulated Phishing Campaigns*. 4105–4122. https://www.usenix.org/conference/usenixsecurity23/presentation/brunken
3. Carney, D. R., Cuddy, A. J. C., & Yap, A. J. (2010). Power Posing: Brief Nonverbal Displays Affect Neuroendocrine Levels and Risk Tolerance. *Psychological Science*, *21*(10), 1363–1368. https://doi.org/10.1177/0956797610383437
4. Cialdini, R. B. (2006). *Influence: The Psychology of Persuasion* (2nd ed.). Harper Business.
5. Cialdini, R. B., Cacioppo, J. T., Bassett, R., & Miller, J. A. (1978). Low-ball procedure for producing compliance: Commitment then cost. *Journal of Personality and Social Psychology*, *36*(5), 463–476. https://doi.org/10.1037/0022-3514.36.5.463
6. Cuddy, A. J. C., Schultz, S. J., & Fosse, N. E. (2018). P-Curving a More Comprehensive Body of Research on Postural Feedback Reveals Clear Evidential Value for Power-Posing Effects: Reply to Simmons and Simonsohn (2017). *Psychological Science*, *29*(4), 656–666. https://doi.org/10.1177/0956797617746749
7. Dang, J., King, K. M., & Inzlicht, M. (2020). Why Are Self-Report and Behavioral Measures Weakly Correlated? *Trends in Cognitive Sciences*, *24*(4), 267–269. https://doi.org/10.1016/j.tics.2020.01.007
8. Distler, V. (2023). The Influence of Context on Response to Spear-Phishing Attacks: An In-Situ Deception Study. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–18. https://doi.org/10.1145/3544548.3581170
9. Ekman, P., & Friesen, W. V. (1969). The Repertoire of Nonverbal Behavior: Categories, Origins, Usage, and Coding. *Semiotica*, *1*(1), 49–98. https://doi.org/10.1515/semi.1969.1.1.49
10. Festinger, L. (1962). *A Theory of Cognitive Dissonance* (Vol. 2). Stanford University Press.
11. Garrison, K. E., Tang, D., & Schmeichel, B. J. (2016). Embodying Power: A Preregistered Replication and Extension of the Power Pose Effect. *Social Psychological and Personality Science*, *7*(7), 623–630. https://doi.org/10.1177/1948550616652209
12. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons, Inc.
13. Jansson, K., & Von Solms, R. (2013). Phishing for phishing awareness. *Behaviour & Information Technology*, *32*(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650
14. Jones, H. S., Towse, J. N., Race, N., & Harrison, T. (2019). Email fraud: The search for psychological predictors of susceptibility. *PLOS ONE*, *14*(1), e0209684. https://doi.org/10.1371/journal.pone.0209684
15. Kim, Y.-H., Kwon, H., Lee, J., & Chiu, C.-Y. (2016). Why Do People Overestimate or Underestimate Their Abilities? A Cross-Culturally Valid Model of Cognitive and Motivational Processes in Self-Assessment Biases. *Journal of Cross-Cultural Psychology*, *47*(9), 1201–1216. https://doi.org/10.1177/0022022116661243
16. Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka (Eds.), *ICT and Society* (Vol. 431, pp. 266–279). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44208-1_22
17. Norton, M. I., Mochon, D., & Ariely, D. (2012). The IKEA effect: When labor leads to love. *Journal of Consumer Psychology*, *22*(3), 453–460. https://doi.org/10.1016/j.jcps.2011.08.002
18. Petty, R. E., & Cacioppo, J. T. (1986). The Elaboration Likelihood Model of Persuasion. In R. E. Petty & J. T. Cacioppo (Eds.), *Communication and Persuasion: Central and Peripheral Routes to Attitude Change* (pp. 1–24). Springer New York. https://doi.org/10.1007/978-1-4612-4964-1_1

# Quellen (2)


19. Plamper, J. (2015). *The History of Emotions: An Introduction*. OUP Oxford.
20. Pronin, E., Lin, D. Y., & Ross, L. (2002). The Bias Blind Spot: Perceptions of Bias in Self Versus Others. *Personality and Social Psychology Bulletin*, *28*(3), 369–381. https://doi.org/10.1177/0146167202286008
21. Ranehill, E., Dreber, A., Johannesson, M., Leiberg, S., Sul, S., & Weber, R. A. (2015). Assessing the Robustness of Power Posing: No Effect on Hormones and Risk Tolerance in a Large Sample of Men and Women. *Psychological Science*, *26*(5), 653–656. https://doi.org/10.1177/0956797614553946
22. Russell, J. A., & Fernández-Dols, J. M. (1997). *The Psychology of Facial Expression*. Cambridge University Press.
23. Sasse, M. A., Hielscher, J., Friedauer, J., & Buckmann, A. (2023). Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, & A. Shukla (Eds.), *Computer Security. ESORICS 2022 International Workshops* (pp. 248–265). Springer International Publishing. https://doi.org/10.1007/978-3-031-25460-4_14
24. Simmons, J. P., & Simonsohn, U. (2017). Power Posing: P-Curving the Evidence. *Psychological Science*, *28*(5), 687–693. https://doi.org/10.1177/0956797616658563
25. Smith, K. M., & Apicella, C. L. (2017). Winners, losers, and posers: The effect of power poses on testosterone and risk-taking following competition. *Hormones and Behavior*, *92*, 172–181. https://doi.org/10.1016/j.yhbeh.2016.11.003
26. Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management*, *34*(4), 1203–1228. https://doi.org/10.1108/JEIM-08-2019-0217
27. Thun, F. S. von. (1981). *Miteinander reden 1: Störungen und Klärungen: Allgemeine Psychologie der Kommunikation*. Rowohlt Verlag GmbH.
28. Tversky, A., & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, *211*(4481), 453–458. https://doi.org/10.1126/science.7455683
29. Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. In I. Boureanu, C. C. Drăgan, M. Manulis, T. Giannetsos, C. Dadoyan, P. Gouvas, R. A. Hallman, S. Li, V. Chang, F. Pallas, J. Pohle, & A. Sasse (Eds.), *Computer Security* (pp. 312–328). Springer International Publishing. https://doi.org/10.1007/978-3-030-66504-3_19
30. Wason, P. C. (1960). On the Failure to Eliminate Hypotheses in a Conceptual Task. *Quarterly Journal of Experimental Psychology*, *12*(3), 129–140. https://doi.org/10.1080/17470216008416717
31. Hielscher, J., Kluge, A., Menges, U., & Sasse, M. A. (2022). "Taking out the Trash": Why Security Behavior Change requires Intentional Forgetting. *Proceedings of the 2021 New Security Paradigms Workshop*, 108–122. https://doi.org/10.1145/3498891.3498902