



What Motivates and Discourages Employees in Phishing Interventions:

An Exploration of Expectancy-Value Theory

Xiaowei CHEN, Sophie DOUBLET, Anastasia SERGEEVA,
Gabriele LENZINI, Vincent KOENIG, University of Luxembourg;
Verena DISTLER, University of the Bundeswehr Munich



A large, semi-transparent image of a hand pulling strings attached to a small figure, symbolizing manipulation, is positioned on the left side of the slide. The hand is at the top left, and the strings extend downwards to a small figure in the center-left area.

**Phishing attacks
use social engineering
techniques to manipulate
recipients, leading to
malicious websites or
download malware.**



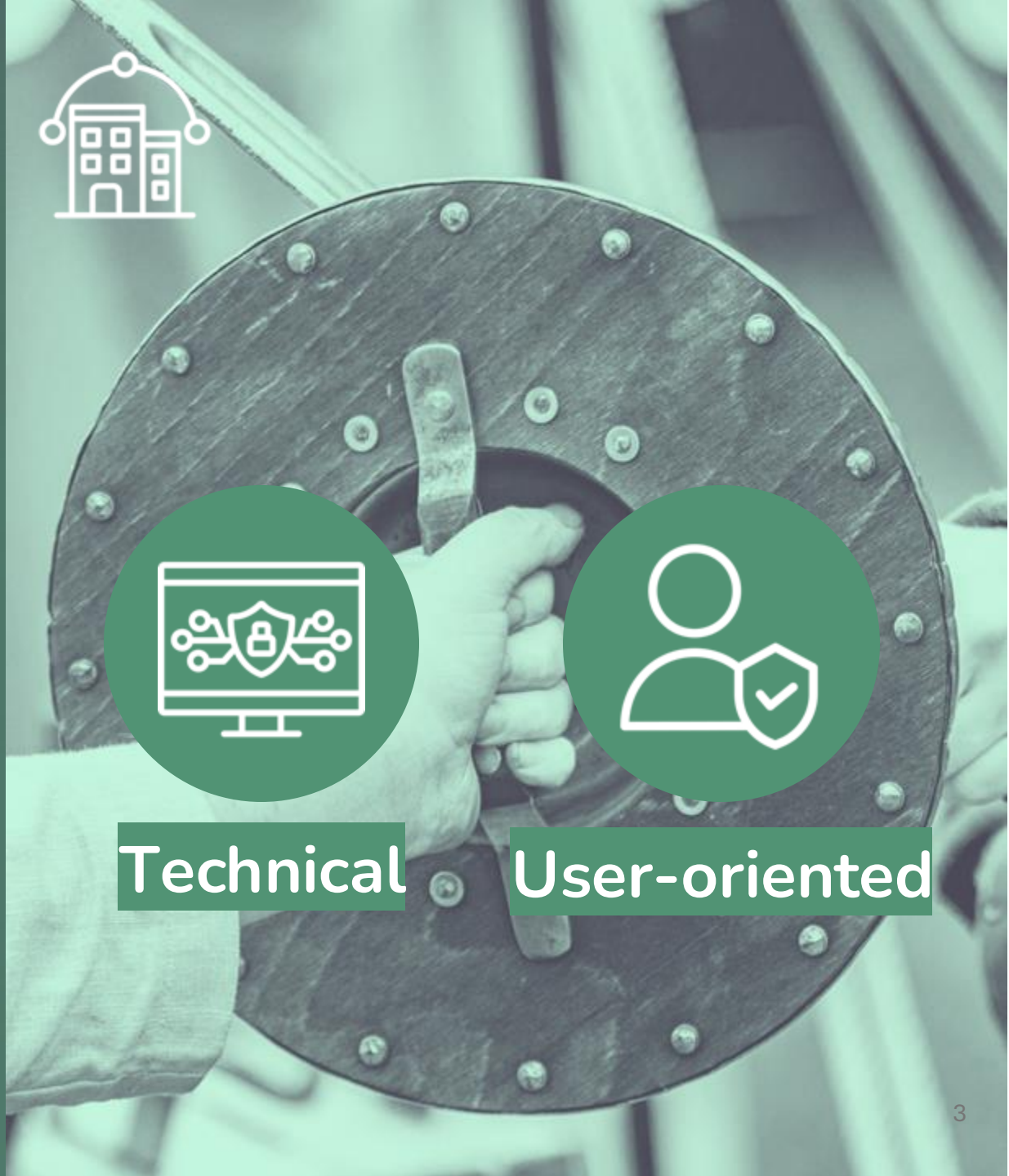
Phishing attacks use social engineering techniques to manipulate recipients, leading to malicious websites or download malware.



Technical



User-oriented





User-oriented

Employees' engagement with these human-oriented interventions often does not meet security experts' expectations.

Phishing awareness campaigns

Online security courses

- **Text, comic, and stories** (Hu et al., 2022), **phishing quizzes** (Weaver et al., 2021)
- **Short phishing awareness videos** (Volkamer et al., 2018)

Simulated phishing tests

- **Education and evaluation purposes** (Hielscher et al., 2023)
- Require resources to deploy and have **side effects** (Rizzoni et al., 2022)
- **Efficacy** of embedded training approach (Lain et al., 2022; Yeoh et al., 2022)

User-oriented



Reporting Phishing emails

- Effective for early detection of threats that bypass technical filters.



Motivators

- ↑ Perceived **self-efficacy**, cybersecurity **self-monitoring** (Kwak et al., 2020)
- ↑ **Subjective norms**, altruism (Marin et al., 2023)
- ↑ Improving **email filters**, and receiving **positive feedback** (Distler, 2023)



Factors discouraging

- ↓ **Uncertainties** regarding the reporting process/rationale and **concerns** about “getting colleagues into trouble” (Distler, 2023)

User-oriented

Research objectives



RQ1

Which factors **motivate** employees to engage with phishing interventions?

RQ2

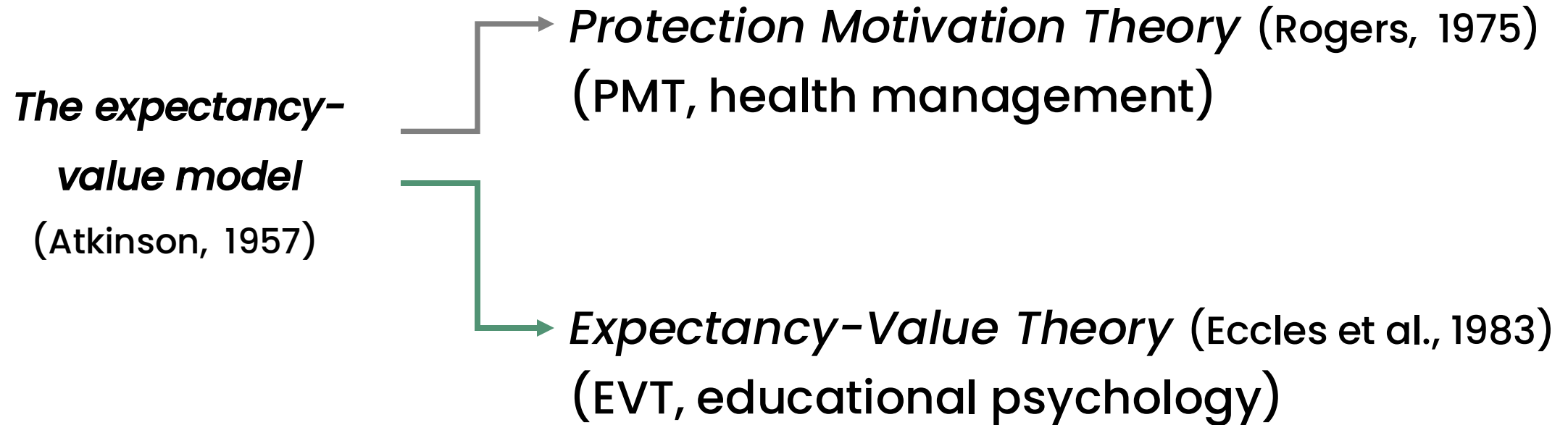
Which factors **discourage** employees from engaging with phishing interventions?

RQ3

From the employees' perspective, which aspects of phishing interventions could be **improved**?

Motivation theories from educational psychology can be useful in explaining employee's (dis-)engagement.

Theoretical model applied in our study



Expectancy-Value Theory (Eccles and Wigfield, 2020)

- **Expectation of success**
- **Subjective task value** (Benefits & Costs)
- **Goals and self-schemata** (Ability, Identity, Self-concept importance, and Goals)

Study Design



7 Focus group
(Exploratory)




34 employees at a European
university

Welcome &
consent



Warm up
activities

 *What motivates /
discourages you?*

Group
discussion

12 questions

- General opinions
- Role identification
- Task value...

+ 

*What motivates /
discourages you
reporting?*

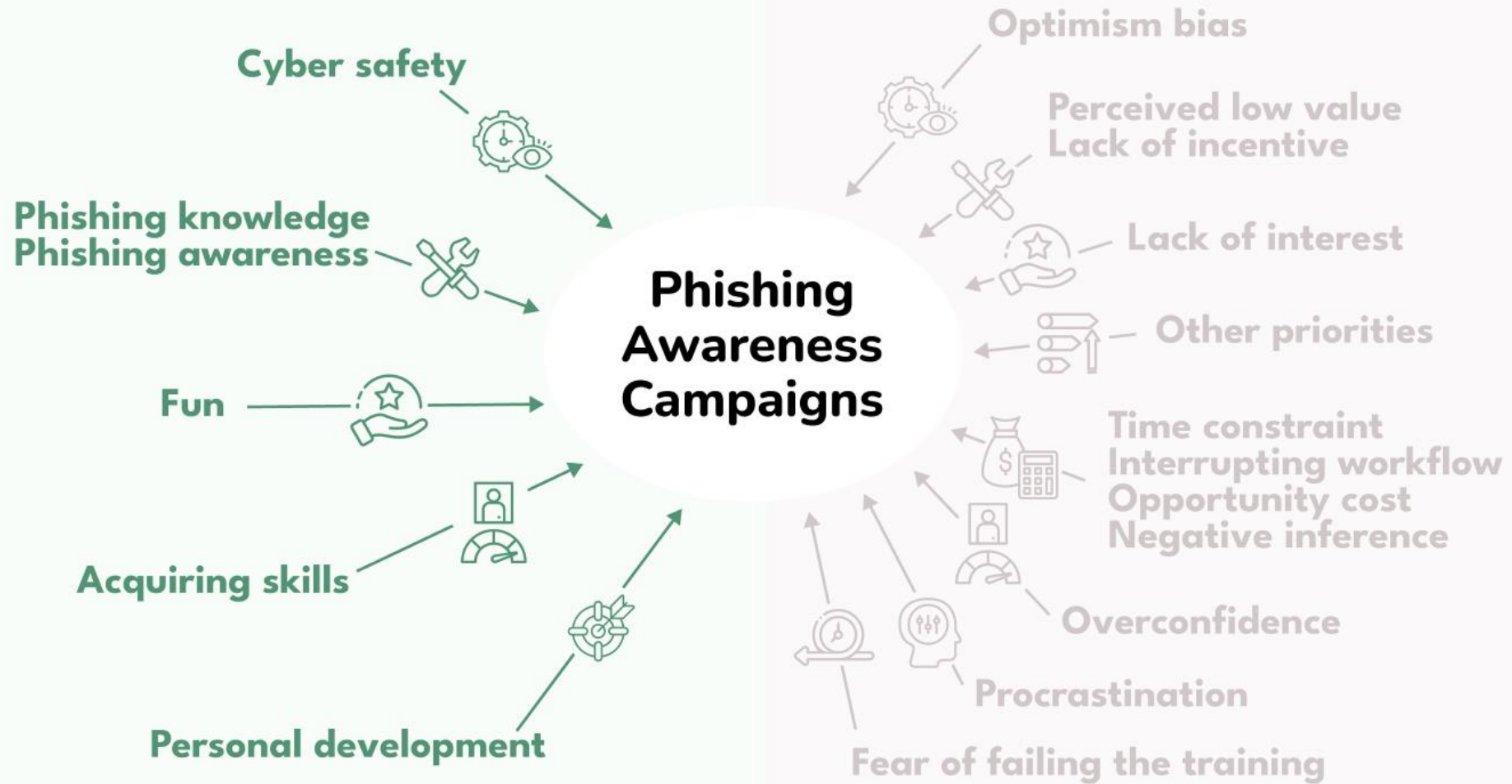
Take the role
of CISO

*What would
you do to
motivate
employees?*

Debriefing

*Standard
practices to
avoid any mis-
understandings*

Factors that motivate





“It’s not only about fear of being attacked...

Everything related to **cybersecurity** is very fundamental now and, in the future, **would become even more fundamental, like reading.**”

Factors that motivate





“The main benefit of reporting is that the IT team could **create more filters** for phishing emails if they have more data (from reporting), **making us safer.**”



“I had this **scam attack**, and I felt bad about myself. I felt bad about trusting the others, so I wouldn't like someone, other people to feel the same way I felt once.”

Factors that discourage





“What is **my incentive** to do an optional course here?”

Factors that discourage





“We don’t know **what the effectiveness** of reporting phishing emails is. We don’t know the numbers, so it would be really good to have **a kind of feedback** status. What has been done last year? What was the success rate?”

Suggestions from employees



Gamification elements



New employees & **Mandatory** training



User experience



Regular **communication** and individual **feedback**



Present **real** incidents



Authentication of internal emails, more IT employees, and punishment approach

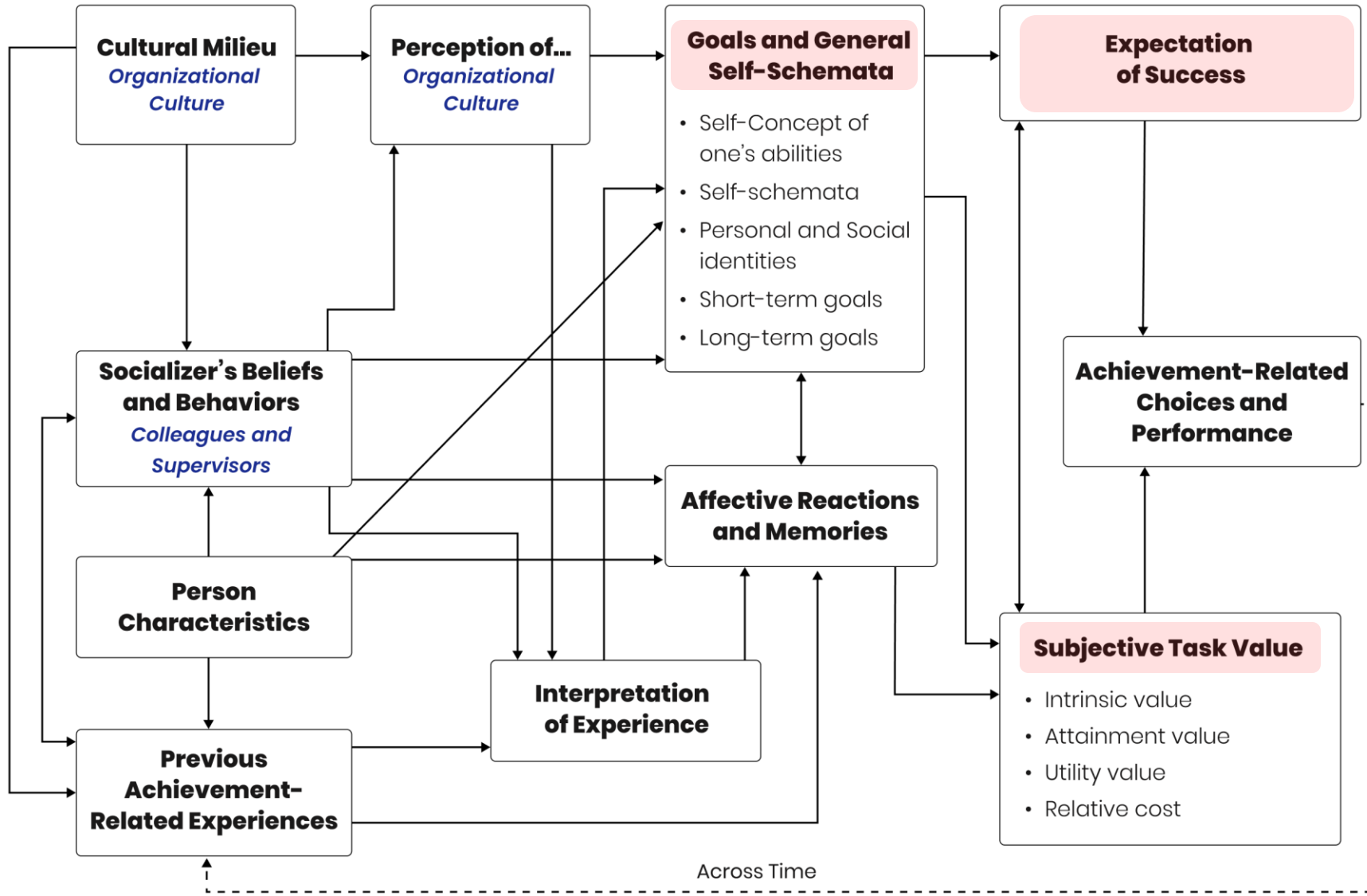


Figure: The expectancy-value model adapted from Eccles and Wigfield (2020).

Key takeaways



EVT framework can be useful in organizational security settings.



Subjective task value influences employees' engagement.



Without **Feedback** and response efficacy, even highly motivated employees might **discourage** from reporting.



The “**interpretation of experience**” can alter goals and subjective task value, influencing “expectation of success”,



Employees are interested in security-related knowledge, linking it with **personal** and **professional growth**.

 **Read our paper**



Reference list:

- ATKINSON J. W. Motivational determinants of risk-taking behavior. *Psychological Review*, 64 (1957). 359–372.
- DISTLER, V. The influence of context on response to spear-phishing attacks: an in-situ deception study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (2023)*, pp. 1–18.
- ECCLES J. S., ADLER, T. F., FUTTERMAN, R., GOFF, S. B., KACZALA, C. M., MEECE, J. L., & MIDGLEY, C. (1983). Expectancies, values, and academic behaviors. In J. T. Spence (Ed.), *Achievement and achievement motivation* (pp. 75–146). San Francisco, CA: W. H. Freeman.
- ECCLES, J. S., AND WIGFIELD, A. From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary educational psychology* 61 (2020), 101859.
- HIELSCHER, J., MENGES, U., PARKIN, S., KLUGE, A., AND SASSE, M. A. “Employees Who Don’t Accept the Time Security Takes Are Not Aware Enough”: The CISO View of Human-Centred Security. In *32nd USENIX Security Symposium (USENIX Security 23) (2023)*, pp. 2311–2328.
- HU, S., HSU, C., AND ZHOU, Z. Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems* 62, 4 (2022), 752–764.
- KWAK, Y., LEE, S., DAMIANO, A., AND VISHWANATH, A. Why do users not report spear phishing emails? *Telematics and Informatics* 48 (2020), 101343.
- LAIN, D., KOSTIAINEN, K., AND APKUN, S. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP) (2022)*, IEEE, pp. 842–859.
- MARIN, I. A., BURDA, P., ZANNONE, N., AND ALLODI, L. The influence of human factors on the intention to report phishing emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (2023)*, pp. 1–18.
- RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., AND COVENTRY, L. Phishing simulation exercise in a large hospital: A case study. *Digital Health* 8 (2022), 20552076221081716.
- ROGERS R. W. A protection motivation theory of fear appeals and attitude change¹. *The journal of psychology*, 91(1) (1975). 93-114.
- VOLKAMER, M., RENAUD, K., REINHEIMER, B., RACK, P., GHIGLIERI, M., MAYER, P., KUNZ, A., AND GERBER, N. Developing and evaluating a five minute phishing awareness video. In *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15 (2018)*, Springer, pp. 119–134
- WEAVER, B. W., BRALY, A. M., AND LANE, D. M. Training users to identify phishing emails. *Journal of Educational Computing Research* 59, 6 (2021), 1169–1183.
- YEOH, W., HUANG, H., LEE, W.-S., AL JAFARI, F., AND MANSSON, R. Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems* 62, 4 (2022), 802–821.

