Big Five Personality Traits and Security Awareness Training Preferences

Isabel K. Glückert, Tobias Fertig, Ricard Bibaj, Sebastian Biedermann

TTZ-WUE Cyber Security - Technical University of Applied Sciences Würzburg-Schweinfurt, Würzburg Germany
isabel.glueckert@thws.de, tobias.fertig@thws.de, ricard.bibaj@thws.de, sebastian.biedermann@thws.de

Individual behavior plays a central role in information security, as many incidents result from user behavior. Accordingly, Information Security Awareness training has become a central measure to support individual security-related decision-making. However, standardized ISA training often shows limited effectiveness, as it rarely accounts for individual differences in learning preferences and motivation. This study examines how personality traits relate to ISA training preferences. A quantitative survey assessed personality using the BFI-2 and collected preference ratings for 18 training methods. Significant relationships were found for Agreeableness and Conscientiousness. Higher Agreeableness was associated with lower preference for socially exposed methods, while individuals high in Conscientiousness preferred structured and practice-oriented methods. The findings suggest that personality shapes how ISA training is perceived and highlight the importance of considering individual differences in the design of training methods. Providing a variety of training methods, rather than a single standardized approach, may improve perceived fit and acceptance.

DOI
https://doi.org/10.18690/um.fov.4.2026.41

ISBN
978-961-299-152-4

Keywords:
information security awareness, big five personality model, training preferences, human factors, personalization

University of Maribor Press

1 Introduction

Information security has become a central organizational challenge in light of increasing digitalization and attack sophistication (BSI, 2024; ENISA, 2024). A substantial share of cybersecurity incidents is attributable to human factors (IBM, 2025; Ugbebor et al., 2024), including compromised legitimate accounts and social engineering attacks exploiting stress, trust, or curiosity (Proofpoint, 2023; Ugbebor et al., 2024). Accordingly, human behavior is a critical determinant of organizational security (Helisch & Pokoyski, 2009; Khadka & Ullah, 2025; Parrish et al., 2009; Schütz, 2018; Weber et al., 2020). To mitigate these risks, organizations rely on Information Security Awareness (ISA) trainings (Bada et al., 2019; BSI, 2024; ENISA, 2024). However, traditional awareness trainings focus on knowledge transfer and often show limited impact on security behavior (Bada et al., 2019; Fertig & Schütz, 2020; Weber et al., 2020). Knowledge alone is insufficient, as individuals behave differently despite comparable knowledge or intentions (Ajzen, 1991). Standardized ISA trainings rarely account for individual differences in motivation and learning styles (Shappie et al., 2020). Personality is a central factor for individual behavioral differences (DeYoung, 2015). Empirical research shows that Big Five personality traits are associated with security-relevant attitudes and behaviors (McCormac et al., 2017; Shappie et al., 2020). Consequently, psychological factors must be considered in awareness training design to achieve long-term improvements in security-relevant behavior (Bada et al., 2019; Fertig & Schütz, 2020; Proofpoint, 2023; Weber et al., 2020). However, it remains unclear how personality traits are reflected in preferences for different ISA training methods. Addressing this gap, this study examines the relationship between the Big Five personality traits and ISA training preferences using a quantitative survey. The focus is on perceived preferences rather than on behavioral outcomes or training effectiveness. This leads to the following research question and hypothesis:

RQ1: How are the Big Five personality traits related to individual preferences for different Information Security Awareness (ISA) training methods in academic and work contexts?

H1: If individuals differ in their Big Five personality traits, they also differ in their preferences for different Information Security Awareness (ISA) training methods.

The paper is structured as follows: Section 2 presents the theoretical foundations and reviews prior research on information security awareness and personality. Section 3 outlines the methodology of the quantitative study. Section 4 reports the results, which are discussed in Section 5. Finally, Section 6 summarizes the key findings and highlights implications for future research.

2 Related Work

Information security is commonly conceptualized through the CIA triad, encompassing confidentiality, integrity, and availability (ISO, 2018). ENISA (2024) defines information security as the interplay of technical, organizational, and human measures to protect information assets. However, security programs remain predominantly technology-oriented and insufficiently consider behavioral factors (ENISA, 2024; Khadka & Ullah, 2025; SANS Institute, 2025). Approximately 85% of cybersecurity incidents are attributable to human errors (Ugbebor et al., 2024). Consequently, end-user behavior plays a central role in preventing cyber-attacks (Prümmer et al., 2024) and ISA has emerged as a distinct research field (Fertig & Schütz, 2020). ISA refers to employees' awareness of security-related risks and their understanding of security rules (Fertig et al., 2022; Richter et al., 2018). The relevance of awareness is particularly evident in phishing, one of the most common attack methods that exploits human errors and cognitive vulnerabilities (2025 Data Breach Investigations Report, 2025; Bada et al., 2019; ENISA, 2024; Schütz, 2018).

2.1 Limitations of Standardized Awareness Training Approaches

Increasing threat complexity places a burden on security professionals, 66% of whom perceive their work as more stressful than in 2020 (ISACA, 2025). Accordingly, organizations invest substantial resources in ISA trainings, recognizing them as a central measure (ENISA, 2024). This growth is reflected in a global ISA training market of USD 4.30 billion in 2023, projected to exceed USD 21 billion by 2032 (Zion Market Research, 2024). Despite these investments, the behavior-changing impact of ISA trainings remains limited (Bada et al., 2019). This is confirmed by large-sample studies reporting only marginal reductions in misclicks and high dropout rates (Ho et al., 2025). This limited effectiveness contributes to ISA trainings being perceived as a formal obligation rather than supportive assistance (Bada et al., 2019; Hornetsecurity GmbH, 2024; SANS Institute, 2025).

Consequently, knowledge-based training approaches have limited influence on security behavior (Bada et al., 2019; Bilal Khan, 2011; Fertig & Schütz, 2020; Proofpoint, 2023; Schütz, 2018; Weber et al., 2020). The failure of classical training approaches to account for individual adaptation has long been recognized (Eighteen, 1999). Accordingly, behavioral change depends on multiple individual factors. A central framework in this context is the Integrated Behavioral Model (IBM), which conceptualizes human behavior as the result of multiple factors (Montaño & Kasprzyk, 2008). In security contexts, the IBM shows that security-compliant actions often fail despite knowledge, while standardized training inadequately addresses employee needs (Schütz, 2018). These findings highlight the need to consider individual differences for sustainable behavioral change (Proofpoint, 2023).

2.2 Learning-Theoretical Foundations of ISA Training

Learning is commonly understood as an active process in which individuals select, organize, and integrate information with prior knowledge to construct new understanding (Jonassen & Rohrer-Murphy, 1999; Mayer, 2002). Information processing occurs through different channels, such as verbal and non-verbal systems (Clark & Paivio, 1991). At the same time, learning is constrained by the limited capacity of working memory. The design of instruction significantly influences the cognitive load of learners, and inappropriate teaching methods can impose additional cognitive burden (Sweller, 2010). In the context of information security, these challenges become particularly evident. Although ISA training methods can improve users' knowledge and attitudes, their impact on actual security-related behavior remains limited (Prümmer et al., 2024) and behavioral outcomes are influenced by individual factors (Schütz, 2018). Against this background, it becomes evident that the selection of appropriate ISA training methods is crucial for learning success and depends on individual characteristics. In information security, where behavioral change often remains limited despite training, it is relevant to examine how personality traits relate to preferences for different ISA training methods.

2.3 Personality as an Influencing Factor on Security Behavior

Personality influences how individuals respond to security-relevant requirements and represents a central leverage point for designing effective ISA training methods (DeYoung, 2015; Shappie et al., 2020). This is partly because personality influences

how individuals learn and process information. People perceive identical situations differently, meaning that the same training experiences are not equally effective for all learners (Chamorro-Premuzic, 2005). Established personality models such as the Big Five have long been used to capture individual differences (Rammstedt & John, 2007). The Big Five model describes five stable traits, Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness, and serves as a framework for explaining individual differences in security-relevant behavior (McCrae & John, 1992; Roccas et al., 2002; Shappie et al., 2020). Empirical findings in the context of learning processes show that Big Five personality traits are related to different learning styles and influence how individuals process information and apply learning strategies (Komarraju et al., 2011). These differences are also reflected in security contexts, where personality traits are associated with security-related attitudes, behavioral intentions, and actual behavior (Grandhi & Still, 2025; McCormac et al., 2017; Shappie et al., 2020; Uffen & Breitner, 2013). Early studies indicate that personality traits, particularly Conscientiousness and Agreeableness, often represent stronger predictors of security-compliant behavior than technology-related attitudes (Shropshire et al., 2006). More recent research considers all five personality traits (Grandhi & Still, 2025; Shappie et al., 2020). These findings indicate that higher Conscientiousness, Agreeableness, and emotional stability are associated with greater security awareness, whereas higher risk propensity shows opposite effects (McCormac et al., 2017). Accordingly, the Big Five model provides a theoretical foundation for explaining individual differences in security-relevant behavior and designing target-group-specific ISA training methods. These individual differences imply that preferences for training methods vary across individuals (Chamorro-Premuzic, 2005) and are reflected in the design of ISA training methods, as different methods provide distinct learning experiences.

2.4 Types and Effectiveness of ISA Training Methods

As personality traits influence learning processes and responses to security requirements (Shappie et al., 2020), the selection of ISA training methods becomes critical. Text-based ISA methods are widely used but show limited effects on security behavior and sustainable change (Bada et al., 2019). Given the increasing importance of digital training methods, e-learning has become a central instrument in organizational training and development (Overton, 2023). Around 91% of organizations rely on technology-supported learning formats, including e-learning

courses, webinars, and learning platforms. These technologies enable flexible, accessible learning independent of time and location (Overton, 2023) and are widely used in organizational information security awareness programs (Fertig et al., 2019). Beyond e-learning, game-based methods foster active participation and perspective-taking, enhancing understanding of social manipulation and phishing (Fatima et al., 2019; Prümmer et al., 2024). Presentation-based methods support structured knowledge transfer (Prümmer et al., 2024; Sykosch et al., 2020). The literature identifies video-based, text-based, and discussion-oriented formats (Prümmer et al., 2024). The evaluation of ISA training preferences forms the study's empirical core.

3 Methodology

This study employed a quantitative research design (Creswell & Creswell, 2018) to examine relationships between Big Five personality traits and ISA training preferences. While qualitative approaches explore individual experiences, this study adopts a quantitative design to identify relationships between personality traits and ISA training preferences across a larger sample. Individual differences are captured through standardized personality measures, enabling comparison of personality profiles. This approach ensures sufficient variability across personality traits and allows identifying generalizable patterns across individuals, which would be difficult to capture using purely qualitative methods. Data were collected via an online survey including the Big Five Inventory-2 (BFI-2) (Soto & John, 2017) and ratings for 18 ISA training methods. Personality was assessed before evaluating ISA training methods to avoid priming effects (Schwarz & Strack, 1991). Big Five traits were treated as independent variables, and training preferences as dependent variables.

3.1 Measurement Instruments and Variables

Participants' personality traits were assessed using the Big Five Inventory-2 (BFI-2), a validated instrument measuring the five traits Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness (Soto & John, 2017). The questionnaire comprises 60 items rated on a five-point Likert scale (Likert, 1932). The analysis was conducted at the trait level, focusing on higher-order personality traits and their relationship with ISA training preferences. Subsequently, ISA training preferences were assessed using a literature-based categorization system distinguishing seven training categories (Prümmer et al., 2024). Based on this

framework and complemented by informal expert consultations, 18 ISA training methods were identified. The consultations involved three practitioners (e.g., IT security managers and awareness specialists) and served to validate the practical relevance and completeness of the selected methods. They were conducted in an exploratory manner without a formal qualitative design. Accordingly, no structured interview protocol or systematic coding procedure was applied. These methods include passive methods such as videos, interactive approaches such as workshops and simulations, and game-based methods such as gamification. The selection of training methods aimed to capture diverse personality profiles and preference patterns. To ensure uniform understanding, each of the 18 ISA training methods was accompanied by a brief standardized description outlining its procedure to minimize bias from differing interpretations. Participants rated their preference for each ISA training method on a five-point Likert scale (1 = not preferred at all to 5 = strongly preferred). The full instrument is provided in Appendix A.

Table 1: Assignment of ISA training methods to categories

Training category	ISA Training methods
Game-based Training	Security competitions, quizzes, gamified learning
Presentation-based Training	Web seminars, expert lectures, awareness-themed days
Simulation-based Training	Simulations, hands-on learning, role plays, case studies
Information-based Training	E-learning platforms, podcasts, mobile learning applications
Video-based Training	Videos
Text-based Training	Documentation
Discussion-based Training	Group work, discussion rounds, mentoring programs

Source: (Prümmer et al., 2024)

3.2 Data Collection and Sample

Data were collected via an online LimeSurvey survey. Participants were recruited via institutional mailing lists, professional networks, and digital channels. Eligible participants had basic experience or regular exposure to IT- and information-security-related topics in academic or work contexts. To ensure meaningful evaluation, a screening question assessed prior experience with learning or training methods in academic or professional contexts. Only participants confirming such

experience proceeded with the survey. This open formulation avoided restricting participation to a specific context and enabled a broader assessment of training preferences. In total, 173 individuals participated. Data cleaning ensured data quality. Incomplete responses were removed, and only fully completed questionnaires without missing values were included. Responses were also screened for plausibility, and datasets with indications of inattentive responding (e.g., uniform response patterns across items or straight-lining) were removed. After data cleaning, a total of 134 valid responses remained for analysis. The sample consisted predominantly of students (80%) and employees from organizations with established ISA training programs (20%). The focus on students is justified, as higher education institutions are more frequently affected by cyberattacks than companies, with 92% reporting incidents compared to 39% of companies (GOV.UK, 2022). Students were enrolled in IT-related degree programs and had experience with IT systems, for example through internships or part-time employment.

4 Results

This section presents empirical results, focusing on relationships between Big Five personality traits and ISA training preferences, including reliability and correlations.

4.1 Reliability and Data Assessment

Internal consistency was assessed using Cronbach's alpha (Cronbach, 1951) for the ISA training items. For the BFI-2 (Soto & John, 2017), established reliability coefficients (.60–.88) were adopted, indicating adequate to good internal consistency (Cronbach, 1951; Danner et al., 2019). For the 18 ISA training items, Cronbach's alpha was .909, indicating excellent internal consistency (Cronbach, 1951). However, this value should be interpreted with caution, as the instrument captures preferences for diverse ISA training methods rather than a unidimensional construct. The high internal consistency may reflect general preference tendencies across training methods and the large number of items. Variable distributions were examined using the Shapiro–Wilk test (Shapiro & Wilk, 1965); significant deviations from normality ($p < .05$) led to the use of Spearman's ϱ for correlation analyses (Spearman, 1904).

4.2 Analysis of Relationships

In total, 90 associations were examined by linking the five Big Five personality traits with the 18 ISA training methods. As the study focuses on preferences for distinct ISA training methods, each method was treated as an individual variable and analyzed using item-level correlation analysis. To examine whether the ISA training methods form underlying dimensions, an exploratory factor analysis was conducted. The results indicated no clear multi-factor structure, as most items loaded on a single dominant factor. This suggests that ISA training preferences reflect general preference tendencies rather than distinct training categories. Therefore, item-level analysis was considered more appropriate to capture specific preference patterns across different training formats. Four significant relationships ($p < .05$) were identified, all relating to Agreeableness and Conscientiousness. Given the large number of tests and the absence of correction for multiple comparisons, some findings may reflect chance. Table 2 summarizes these relationships. No statistically significant associations were identified for Openness, Extraversion, or Neuroticism ($p \geq .05$). Agreeableness was negatively associated with preferences for web seminars ($r = -.177$, $p = .041$) and role plays ($r = -.186$, $p = .031$). In contrast, Conscientiousness was positively associated with preferences for hands-on learning ($r = .246$, $p = .004$) and documentation ($r = .190$, $p = .028$). These results suggest that structured and practice-oriented ISA training methods are preferred by conscientious individuals. With regard to H1, relationships between personality traits and ISA training preferences were observed only for Agreeableness and Conscientiousness, with no effects for Openness, Extraversion, or Neuroticism. The results do not support H1 but indicate selective personality–preference relationships.

Table 2: Significant ISA training–personality correlations

	Agreeableness (mean)	Conscientiousness (mean)
Web seminar	r = -.177; p = .041	-
Role play	r = -.186; p = .031	-
Hands-on learning	-	r = .246; p = .004
Documentation	-	r = .190; p = .028

5 Discussion

Overall, four examined relationships are empirically relevant and associated with preferences for specific ISA training methods, exclusively concerning Agreeableness and Conscientiousness. The discussion therefore focuses on subjective preferences rather than observed behavior or the effectiveness of the ISA training methods.

5.1 Personality-Specific Preference Patterns for ISA Training Methods

For Agreeableness, negative relationships were observed with web seminars and role plays. In this study, web seminars are characterized by online content delivery with limited interaction. In contrast, role plays require active participation, social interaction, and enactment of typical situations (Martin et al., 2014; Sheets, 1998). The lower preference of agreeable individuals suggests that training methods involving mandatory participation or increased social visibility are perceived as less suitable. At first glance, this pattern contradicts the definition of Agreeableness (John & Srivastava, 1999), but it can be explained by considering different levels of analysis. Shappie et al. (Shappie et al., 2020) show that Agreeableness is associated with security-relevant behavior. Accordingly, agreeable individuals tend to comply with rules and display protective behavior toward policies, data, and systems (Shappie et al., 2020). In contrast to these behavior-based findings (Shappie et al., 2020), the present study indicates that agreeable individuals perceive ISA training methods with high social exposure, such as role plays or interactive live training, as less suitable. This lower preference can be interpreted as a desire for harmony and reduced social visibility rather than as a lack of willingness to engage in security-compliant behavior. For Conscientiousness, positive relationships emerge with practice-oriented and structuring ISA training methods, particularly hands-on learning and documentation. In the context of this study, hands-on learning refers to training approaches in which security-relevant content is conveyed through direct application of tasks. Documentation refers to written informational materials that present content in a structured, comprehensible, and accessible manner. Within the Big Five model, Conscientiousness is associated with organization, sense of duty, self-discipline, and goal-directed behavior (John & Srivastava, 1999). Moreover, current research shows that Conscientiousness plays a central role in relation to security-relevant behavior (Shappie et al., 2020). Such behavior manifests in rule compliance, regular software updates, and secure password use (Gratian et al., 2018).

Against this background, it is plausible that individuals with high Conscientiousness prefer ISA training methods that are clearly structured, provide concrete guidance for action, and enable direct implementation. These findings suggest that structured and practice-oriented ISA training methods align well with conscientious individuals. These methods cater to a preference for order and clarity. They also facilitate the sustainable integration of security-relevant content into everyday work practices.

5.2 Non-significant Findings, Limitations, and Implications

No significant relationships were found for Openness, Extraversion, and Neuroticism, although these personality traits are commonly associated with social interaction, emotional reactivity, and openness to new experiences (John & Srivastava, 1999). Accordingly, effects on the evaluation of interactive training methods might have been expected. However, the absence of such effects can be interpreted in light of prior research. The Theory of Planned Behavior highlights the gap between behavioral intentions and actual behavior (Ajzen, 1991; Shappie et al., 2020). Personality may influence security-related behavior without being reflected in subjective training preferences. The exploratory factor analysis further refines this interpretation, as ISA training preferences did not form clearly distinguishable categories. This suggests that participants evaluate training formats more holistically. Consequently, personality-based adaptation should focus on specific training methods rather than relying solely on broad training categories. Several limitations must be considered. First, the study relies on self-reported preferences, and not all participants had comparable experience with the evaluated training methods. As a result, some assessments may be based on expectations rather than experience, and preferences do not allow conclusions about training effectiveness. Second, a large number of relationships were tested, while only a few reached statistical significance, indicating that some findings may be due to chance. Third, the sample consisted predominantly of students, limiting generalizability to organizational contexts. Future studies should include working professionals. These limitations underline the need to complement preference-based measurements with behavior-oriented research designs. This study contributes to information security research by linking personality traits to training preferences, thereby extending prior research beyond behavioral outcomes. While prior research primarily focuses on behavioral outcomes, this study takes an earlier step by examining which training methods are preferred by individuals with different personality profiles. This provides a basis for

selecting and designing ISA training methods. From an educational perspective, these findings suggest that considering individual differences allows ISA training methods to be more closely aligned with learners' preferences and needs. This may increase perceived fit, acceptance of training, and motivation. Given the gap between knowledge, attitudes, and behavior in information security (Schütz, 2018), individualized training methods may help bridge this gap and support more targeted ISA training. Based on these findings, two directions for future research emerge. First, qualitative studies could provide deeper insights into the underlying evaluation processes by examining which characteristics are perceived as suitable or unsuitable by different personality types. These insights can inform the design of more effective ISA training. Second, future research should move beyond preference-based analyses and examine the actual effectiveness of ISA training methods by comparing personality-aligned and non-aligned training methods. This comparison could assess whether aligned formats lead to more positive perceptions, higher engagement, improved knowledge retention, and more stable security-related behavior.

6 Conclusion

This study examined how Big Five personality differences are reflected in preferences for ISA training methods. The results show that preference patterns are meaningful only for Agreeableness and Conscientiousness. Higher Agreeableness was associated with lower preference for web seminars and role plays, while Conscientiousness was associated with structured and practice-oriented ISA training methods such as hands-on learning and documentation. These findings indicate that personality traits shape how ISA training methods are evaluated. The results should be interpreted as exploratory and hypothesis-generating. No significant relationships were found for Openness, Extraversion, and Neuroticism, suggesting that personality differences do not consistently translate into preferences. Overall, this study contributes to information security research by examining the link between personality and ISA training preferences, showing that effects are selective rather than uniform. For practice, the findings suggest that ISA training methods should not be designed as a single standardized format, but rather that a variety of ISA training methods should be provided. Taking personality-specific preferences into account may improve perceived fit and acceptance of trainings, thereby supporting motivation and participation. At the same time, it must be emphasized that preferences do not allow conclusions about the effectiveness of a given method, but

indicate which ISA training methods are perceived as suitable by specific target groups. Future research should examine whether these differences are reflected in the effectiveness of ISA training methods, for example through field studies. Studies capturing knowledge acquisition, engagement and security-relevant behavior would be valuable. Overall, sustainable information security cannot be achieved solely through technical measures or standardized training. Instead, it requires considering individual differences in how ISA training methods are perceived and evaluated.

References

2025 Data Breach Investigations Report. (2025). Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, Theories of Cognitive Self-Regulation, 50, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? (arXiv:1901.02672). arXiv. https://doi.org/10.48550/arXiv.1901.02672

Bilal Khan. (2011). Effectiveness of information security awareness methods based on psychological theories. AFRICAN JOURNAL OF BUSINESS MANAGEMENT, 5(26). https://doi.org/10.5897/AJBM11.067

BSI. (2024, November 12). Die Lage der IT-Sicherheit in Deutschland 2024. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html?nn=132646

Chamorro-Premuzic, T. (with Furnham, A.). (2005). Personality and intellectual competence. L. Erlbaum Associates. https://doi.org/10.4324/9781410612649

Clark, J. M., & Paivio, A. (1991). Dual coding theory and education. Educational Psychology Review, 3(3), 149–210. https://doi.org/10.1007/BF01320076

Creswell, J. W., & Creswell, J. D. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (fifth Edition). Sage Publications.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297–334. https://doi.org/10.1007/BF02310555

Danner, D., Rammstedt, B., Bluemke, M., Lechner, C., Berres, S., Knopf, T., Soto, C. J., & John, O. P. (2019). Das Big Five Inventar 2: Validierung eines Persönlichkeitsinventars zur Erfassung von 5 Persönlichkeitsdomänen und 15 Facetten. Diagnostica, 65(3), 121–132. https://doi.org/10.1026/0012-1924/a000218

DeYoung, C. G. (2015). Cybernetic Big Five Theory. Journal of Research in Personality, Integrative Theories of Personality, 56, 33–58. https://doi.org/10.1016/j.jrp.2014.07.004

Eighteen, R. (1999). Training needs analysis for IT training. Industrial and Commercial Training, 31(4), 149–153. https://doi.org/10.1108/00197859910275773

ENISA. (2024, September 19). ENISA Threat Landscape 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. Journal of Computer Security, 27(6), 581–612. https://doi.org/10.3233/JCS-181253

Fertig, T., & Schütz, A. (2020, Januar 7). About the Measuring of Information Security Awareness: A Systematic Literature Review. https://doi.org/10.24251/HICSS.2020.798

Fertig, T., Schütz, A. E., Weber, K., & Müller, N. H. (2019). Measuring the Impact of E-Learning Platforms on Information Security Awareness. In P. Zaphiris & A. Ioannou (Hrsg.), Learning and Collaboration Technologies. Designing Learning Experiences (S. 26–37). Springer International Publishing. https://doi.org/10.1007/978-3-030-21814-0_3

Fertig, T., Schütz, A., & Weber, K. (2022, Januar 4). Automated Measuring of Information Security Related Habits. Hawaii International Conference on System Sciences (HICSS). https://doi.org/10.24251/HICSS.2022.925

GOV.UK. (2022, Juli 11). Educational institutions findings annex—Cyber Security Breaches Survey 2022. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022

Grandhi, S. R., & Still, J. D. (2025). The Big Five in Action: A Systematic Review of Personality, Cyber Awareness, and Behaviors. In A. Moallem (Hrsg.), HCI for Cybersecurity, Privacy and Trust (S. 17–34). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-92833-8_2

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. Computers & Security, 73, 345–358. https://doi.org/10.1016/j.cose.2017.11.015

Helisch, M., & Pokoyski, D. (Hrsg.). (2009). Security Awareness. Vieweg+Teubner. https://doi.org/10.1007/978-3-8348-9594-3

Ho, G., Mirian, A., Luo, E., Tong, K., Lee, E., Liu, L., Longhurst, C. A., Dameff, C., Savage, S., & Voelker, G. M. (2025). Understanding the Efficacy of Phishing Training in Practice. 2025 IEEE Symposium on Security and Privacy (SP), 37–54. https://doi.org/10.1109/SP61157.2025.00076

Hornetsecurity GmbH. (2024, Juni 3). Umfrage zur Security Awareness: 1 von 4 (25,7 %) Unternehmen bietet kein Security Awareness Training an. Hornetsecurity. https://www.hornetsecurity.com/de/blog/security-awareness-umfrage-2024/

IBM. (2025). X-Force 2025 Threat Intelligence Index | IBM. https://www.ibm.com/reports/threat-intelligence

ISACA. (2025, September 29). State of Cybersecurity 2025. ISACA. https://www.isaca.org/resources/reports/state-of-cybersecurity-2025

ISO. (2018, Februar). ISO/IEC 27000:2018. ISO. https://www.iso.org/standard/73906.html

John, O. P., & Srivastava, S. (1999). The Big Five Trait taxonomy: History, measurement, and theoretical perspectives. In Handbook of personality: Theory and research, 2nd ed (2nd ed., S. 102–138). Guilford Press.

Jonassen, D. H., & Rohrer-Murphy, L. (1999). Activity theory as a framework for designing constructivist learning environments. Educational Technology Research and Development, 47(1), 61–79. https://doi.org/10.1007/BF02299477

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Komarraju, M., Karau, S. J., Schmeck, R. R., & Avdic, A. (2011). The Big Five personality traits, learning styles, and academic achievement. Personality and Individual Differences, 51(4), 472–477. https://doi.org/10.1016/j.paid.2011.04.019

Likert, R. (1932). A technique for the measurement of attitudes. Archives of Psychology, 22 140, 1–55.

Martin, B. O., Kolomitro, K., & Lam, T. C. M. (2014). Training Methods: A Review and Analysis. Human Resource Development Review, 13(1), 11–35. https://doi.org/10.1177/1534484313497947

Mayer, R. E. (2002). Multimedia learning. In Psychology of Learning and Motivation (Bd. 41, S. 85–139). Academic Press. https://doi.org/10.1016/S0079-7421(02)80005-6

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

McCrae, R. R., & John, O. P. (1992). An Introduction to the Five-Factor Model and Its Applications. Journal of Personality, 60(2), 175–215. https://doi.org/10.1111/j.1467-6494.1992.tb00970.x

Montaño, D. E., & Kasprzyk, D. (2008). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. In Health behavior and health education: Theory, research, and practice, 4th ed (S. 67–96). Jossey-Bass/Wiley.

Overton, L. (2023). Learning at work 2023 survey report. https://www.cipd.org/globalassets/media/knowledge/knowledge-hub/reports/2023-pdfs/2023-learning-at-work-survey-report-8378.pdf

Parrish, J. L., Bailey, J. L., & Courtney, J. F. (2009). A Personality Based Model for Determining Susceptibility to Phishing Attacks. 285–296.

Proofpoint. (2023, Juni 14). Der Faktor Mensch 2025. Proofpoint. https://www.proofpoint.com/de/resources/threat-reports/human-factor-social-engineering

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Rammstedt, B., & John, O. P. (2007). Measuring personality in one minute or less: A 10-item short version of the Big Five Inventory in English and German. Journal of Research in Personality, 41(1), 203–212. https://doi.org/10.1016/j.jrp.2006.02.001

Richter, S., Straub, T., & Lucke, C. (2018, September 6). Information Security Awareness – eine konzeptionelle Neubetrachtung. Multikonferenz Wirtschaftsinformatik 2018 (MKWI).

Roccas, S., Sagiv, L., Schwartz, S. H., & Knafo, A. (2002). The Big Five Personality Factors and Personal Values. https://doi.org/10.1177/0146167202289008

SANS Institute. (2025). 2025 Security Awareness Report. SANS Institute. https://www.sans.org/mlp/ssa-security-awareness-report

Schütz, A. (2018, Mai 17). Information Security Awareness: It's Time to Change Minds! ICDDAt: Sibiu, Romania. International Conference on Applied Informatics (ICAI).

Schwarz, N., & Strack, F. (1991). Context Effects in Attitude Surveys: Applying Cognitive Theory to Social Research. European Review of Social Psychology, 2(1), 31–50. https://doi.org/10.1080/14792779143000015

Shapiro, S. S., & Wilk, M. B. (1965). An analysis of variance test for normality (complete samples)†. Biometrika, 52(3–4), 591–611. https://doi.org/10.1093/biomet/52.3-4.591

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2020). Personality as a predictor of cybersecurity behavior. Psychology of Popular Media, 9(4), 475–480. https://doi.org/10.1037/ppm0000247

Sheets, J. (1998). Role-Playing as a Training Tool for Reference Student Assistants. Reference Services Review, 26(1), 37–41. https://doi.org/10.1108/00907329810307425

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. 6, 415.

Soto, C. J., & John, O. P. (2017). The next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. Journal of Personality and Social Psychology, 113(1), 117–143. https://doi.org/10.1037/pspp0000096

Spearman, C. (1904). The proof and measurement of association between two things. The American Journal of Psychology, 15(1), 72–101. https://doi.org/10.2307/1412159

Sweller, J. (2010). Element Interactivity and Intrinsic, Extraneous, and Germane Cognitive Load. Educational Psychology Review, 22(2), 123–138. https://doi.org/10.1007/s10648-010-9128-5

Sykosch, A., Doll, C., Wübbeling, M., & Meier, M. (2020). Generalizing the phishing principle: Analyzing user behavior in response to controlled stimuli for IT security awareness assessment. Proceedings of the 15th International Conference on Availability, Reliability and Security, ARES '20, 1–10. https://doi.org/10.1145/3407023.3409205

Uffen, J., & Breitner, M. H. (2013). Management of Technical Security Measures: An Empirical Examination of Personality Traits and Behavioral Intentions. International Journal of Social and Organizational Dynamics in IT (IJSODIT), 3(1), 14–31. https://doi.org/10.4018/ijsodit.2013010102

Ugbebor, F., Aina, O., Abass, M., & Kushanu, D. (2024). EMPLOYEE CYBERSECURITY AWARENESS TRAINING PROGRAMS CUSTOMIZED FOR SME CONTEXTS TO REDUCE HUMAN-ERROR RELATED SECURITY INCIDENTS. Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (Online), 3(3), 382–409. https://doi.org/10.60087/jklst.vol3.n3.p382-409

Weber, K., Schütz, A. E., Fertig, T., & Müller, N. H. (2020). Exploiting the Human Factor: Social Engineering Attacks on Cryptocurrency Users. In P. Zaphiris & A. Ioannou (Hrsg.), Learning and Collaboration Technologies. Human and Technology Ecosystems (S. 650–668). Springer International Publishing. https://doi.org/10.1007/978-3-030-50506-6_45

Zion Market Research. (2024). Cybersecurity Awareness Training Market Size, Share, Analysis, Trends, Growth, Forecasts, 2032. Zion Market Research. https://www.zionmarketresearch.com/report/cybersecurity-awareness-training-market?utm.com

Appendix A: Preferences for ISA Training Methods Instrument

In the following, different training methods in the field of information security are presented. Please indicate for each method how much you would personally prefer to participate in this type of training.

Please try to imagine that you are required to complete such a training as part of your studies or work.

Please evaluate each training method using the following scale:

1 = Not preferred at all
2 = Rather not preferred
3 = Neutral
4 = Rather preferred
5 = Strongly preferred

Table 3: Preferences for ISA Training Methods Instrument

	Description
Security competitions	You participate in a competition where you solve tasks related to IT security, such as identifying vulnerabilities or detecting attacks. You compete with other participants and compare your results.
Quizzes	You answer questions about IT security, for example in the form of short tests or multiple-choice questions. You receive immediate feedback on whether your answers are correct or incorrect.
Gamified learning	You learn IT security content in a game-like environment, for example by collecting points, unlocking levels, or completing small challenges within a learning platform.
Web seminars	You participate in an online session where IT security topics are explained. You mainly listen but may also ask questions or interact via chat.
Expert lectures	You listen to an expert presenting IT security topics, such as current threats or common mistakes in handling data.
Awareness-themed days	You participate in an event dedicated to IT security, which may include different formats such as presentations, short exercises, or informational sessions throughout the day.
Simulations	You are placed in a realistic situation, for example receiving a suspicious email, and must decide how to respond.
Hands-on learning	You actively work on tasks yourself, such as identifying phishing emails, configuring security settings, or applying specific security measures.
Role plays	You act out a situation together with others, for example a conversation with someone trying to obtain confidential information.
Case studies	You analyze a real or realistic security incident and reflect on what happened and how it could have been handled.
E-learning platforms	You use an online platform with structured IT security courses that you can complete independently.
Podcasts	You listen to audio content about IT security, such as interviews or discussions on relevant topics.
Mobile learning applications	You use a mobile app to learn IT security content in short, flexible learning units.
Videos	You watch videos that explain or demonstrate IT security topics.
Documentation	You read written materials such as guidelines, manuals, or wiki pages related to IT security.
Group work	You work together with others on tasks or topics related to IT security and exchange ideas within a team.
Discussion rounds	You participate in discussions where experiences and opinions about IT security are shared.
Mentoring programs	You are guided by an experienced person who provides individual support and shares knowledge about IT security.