International Journal of Education, Vocational and Social Science
https://e-journal.citakonsultindo.or.id/index.php/IJEVSS
E-ISSN : 2963 4954
IJEVSS

Cybersecurity Awareness and AI-Generated Visual Manipulation Detection Ability Among University Students

Muhammad Sulthan Nabil Tursilo
Indonesia University of Education
Nuur Wachid Abdul Majid
Indonesia University of Education

Corresponding Author: *12 sulthannabil1103@upi.edu, nuurwachid@upi.edu

Abstract

This study examines cybersecurity awareness and synthetic image detection ability among 99 students from the Information Systems and Technology Education Study Program at Universitas Pendidikan Indonesia using a quantitative associative-comparative design. Instruments included a 24-item Likert scale questionnaire and a 10-stimulus visual detection test. Results showed high awareness across all dimensions (M = 4.05–4.64), yet detection accuracy reached only 67.0%. No significant relationship was found between awareness dimensions and detection ability, though a significant negative correlation emerged between conceptual understanding and protective behavior (rs = -0.206, p = 0.041). Mann-Whitney U tests revealed a significant gender difference in risk awareness (p = 0.027). Findings highlight a gap between self-reported awareness and actual detection ability, underscoring the need for simulation-based practical training in higher education.The rapid development of artificial intelligence technologies has increased the spread of synthetic visual content and deepfake-based misinformation across digital platforms. Although students demonstrated high cybersecurity awareness, their practical ability to identify manipulated images remained moderate. This finding indicates that theoretical understanding and self-reported digital security behavior do not automatically translate into accurate detection skills. The study emphasizes the importance of strengthening practical digital literacy through hands-on training, visual analysis exercises, and simulation-based cybersecurity education. Integrating these approaches into higher education learning systems may improve students' critical thinking, digital verification skills, and resilience against AI-generated misinformation in increasingly complex online environments.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Keywords: *cybersecurity, deepfake, generative AI, detection ability, cybersecurity awareness*

INTRODUCTION

The emergence of generative AI-based visual manipulation technologies has become one of the most critical cybersecurity challenges within the contemporary digital ecosystem. These technologies encompass a broad spectrum of techniques, ranging from digitally altered facial identity replacement (deepfake) to the synthesis of entirely artificial yet photorealistic human images, collectively generating substantial risks related to visual misinformation, identity abuse, reputational harm, fraud, and privacy violations (Chesney & Citron, 2019; Vaccari & Chadwick, 2020; Westerlund, 2019). In this study, generative AI-based visual manipulation is employed as an umbrella term referring to various artificial intelligence-driven techniques used to synthesize, modify, or fabricate digital visual content, with deepfake representing the most socially impactful and extensively studied manifestation, thus serving as the primary measurement context.

Recent advancements in generative adversarial networks (GANs), diffusion models, and neural rendering systems have significantly increased the realism and accessibility of manipulated visual content. Unlike conventional image editing techniques, generative AI systems are capable of producing highly convincing synthetic media that closely imitate authentic human expressions, voices, and behavioral patterns (Goodfellow et al., 2014; Mirsky & Lee, 2021). The democratization of generative AI platforms further amplifies the threat landscape, as users without advanced technical expertise can now create sophisticated deepfake content through publicly available applications and online services (Kietzmann et al., 2020). Consequently, the challenge posed by AI-generated manipulation extends beyond technological detection systems and increasingly affects human cognitive judgment and trust formation in digital environments.

Within the Indonesian context, the urgency of this issue is intensified by the exceptionally high level of internet penetration among younger populations. According to Statistics Indonesia (Badan Pusat Statistik [BPS], 2024), internet penetration among Generation Z reached 87.80%, while individuals with higher education attainment demonstrated an even higher penetration rate of 91.27%. These figures indicate that university students constitute one of the most digitally connected demographic groups in Indonesia and are continuously exposed to large volumes of visual information through social media platforms such as Instagram, TikTok, X, and YouTube. High-frequency exposure to algorithmically distributed visual content substantially increases the probability of encountering manipulated media, particularly in environments characterized by rapid information consumption and limited verification behavior.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

The risks associated with AI-generated manipulation are not limited to misinformation alone. Previous studies demonstrate that deepfake technologies can facilitate identity theft, political propaganda, financial fraud, cyberbullying, sextortion, and non-consensual explicit content generation (Citron & Chesney, 2019; Paris & Donovan, 2019). Scholars have also warned that deepfake dissemination may contribute to the "liar's dividend," a phenomenon in which genuine evidence becomes easier to dismiss as fabricated, thereby undermining public trust in authentic digital information (Chesney & Citron, 2019). This erosion of epistemic trust presents a serious cybersecurity and societal challenge, particularly among digitally active populations who heavily rely on visual content as a source of information and social interaction.

Despite their intensive internet usage, individuals frequently lack adequate cybersecurity literacy and visual verification competencies. Empirical evidence indicates that people often struggle to distinguish authentic visual content from AI-generated manipulations, particularly when visual realism is high and contextual cues are limited (Groh et al., 2022; Nightingale & Farid, 2022). Human vulnerability to manipulated media is influenced not only by insufficient technical knowledge but also by cognitive biases, heuristic processing, emotional engagement, and the tendency to trust visually persuasive information (Pennycook & Rand, 2021). In many cases, repeated exposure to manipulated content may normalize synthetic media and reduce skepticism toward questionable visual information.

Psychological inoculation theory has emerged as one promising approach for strengthening resilience against manipulative digital content. The inoculation framework suggests that exposing individuals to weakened forms of misinformation alongside refutational strategies can improve resistance against future manipulation attempts (McGuire, 1964; Roozenbeek et al., 2022). Several experimental studies have demonstrated that prebunking and media literacy interventions can enhance users' ability to critically evaluate misleading online content, including deepfake videos and AI-generated misinformation (Basol et al., 2021). However, the effectiveness of such interventions strongly depends on accurate baseline assessments regarding individuals' cybersecurity awareness, digital behavior, and actual detection capabilities.

The relevance of this issue is reflected in real-world incidents occurring within Indonesian universities. One prominent case involved a student at Universitas Udayana who used AI-based deepfake technology to manipulate photographs of female students obtained from Instagram into explicit content, causing psychological trauma to at least 37 victims and resulting in the perpetrator's permanent expulsion from the university. This incident illustrates that AI-generated visual manipulation is no longer a hypothetical cybersecurity concern but a tangible threat

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

affecting privacy, mental health, and digital safety within educational institutions. The case also highlights the urgent need for structured cybersecurity literacy programs capable of addressing emerging AI-related risks among university students.

Although research on deepfake detection, AI-generated misinformation, and cybersecurity awareness continues to expand globally, significant research gaps remain within the Indonesian context. Existing studies predominantly focus either on technical detection systems or self-reported digital literacy assessments, while limited attention has been devoted to integrating subjective cybersecurity awareness measurements with objective detection performance within a unified analytical framework (Groh et al., 2022; Mirsky & Lee, 2021). Furthermore, empirical evidence specifically examining Indonesian university students remains scarce, despite their high level of exposure to social media ecosystems where manipulated visual content proliferates rapidly.

Another important limitation in previous research lies in the discrepancy frequently observed between perceived competence and actual detection ability. Individuals may report high confidence in identifying manipulated media while simultaneously demonstrating poor performance during objective verification tasks (Nightingale & Farid, 2022). This gap between perceived and actual competence has substantial implications for cybersecurity education because overconfidence may reduce individuals' motivation to verify suspicious content. Therefore, combining perception-based awareness assessment with objective detection measurement provides a more comprehensive understanding of cybersecurity readiness in the context of AI-generated threats.

Based on these gaps, this study aims to: (1) measure university students' cybersecurity awareness in terms of conceptual understanding, risk awareness, and protective digital behavior; (2) identify students' actual ability to detect generative AI-based visual manipulation content; (3) analyze the relationships among cybersecurity awareness dimensions and their association with detection performance; and (4) formulate empirically grounded mitigation recommendations to support the development of cybersecurity literacy programs in higher education institutions.

This study is expected to contribute theoretically through the adaptation of contemporary cybersecurity awareness frameworks (Parsons et al., 2017; Zwilling et al., 2022; Tsohou et al., 2015) into the domain of generative AI-based visual manipulation, extending the foundational conceptual model proposed by Kruger and Kearney (2006). Methodologically, the study contributes by implementing a dual-measurement approach that integrates self-reported awareness instruments with objective visual manipulation detection tasks, thereby addressing

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

limitations commonly found in single-method cybersecurity awareness studies. Practically, the findings are expected to provide evidence-based recommendations for universities, policymakers, and cybersecurity educators in designing targeted interventions aimed at strengthening digital resilience against emerging AI-driven threats.

RESEARCH METHODOLOGY

This study employed a quantitative approach with a non-experimental associative–comparative design to examine the relationship between cybersecurity awareness and the ability to detect AI-generated visual manipulation among university students. The associative approach was used to analyze the relationship between cybersecurity awareness dimensions and visual detection ability using the Spearman correlation test, while the comparative approach was applied to identify gender differences through the Mann–Whitney U test. This design was selected because it enables the systematic description of empirical conditions without implementing intervention or treatment (Creswell & Creswell, 2018). The population consisted of active students from semesters 4, 6, and 8 in the Information Systems and Technology Education Program (PSTI) at Universitas Pendidikan Indonesia, with a total population of 214 students. Purposive sampling was applied using several criteria, including active social media usage and willingness to participate in the visual detection test. A total of 99 students participated voluntarily, which may indicate the possibility of non-response bias (Etikan et al., 2016).

The study used two research instruments to reduce self-report bias and provide comprehensive findings. The first instrument was a cybersecurity awareness questionnaire adapted from the framework developed by Kruger and Kearney (2006), consisting of 24 Likert-scale items covering conceptual understanding of deepfake technology, cybersecurity risk awareness, and digital protective behavior. The second instrument was an AI-generated visual detection test consisting of 10 visual stimuli: five authentic images from Unsplash and five synthetic images generated using StyleGAN2 from ThisPersonDoesNotExist.com. Participants classified each image as authentic or synthetic as a proxy measure of visual manipulation literacy (Vaccari & Chadwick, 2020). A summary of the operationalisation of the variables is presented in Table 1.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Table 1. Operationalization of Research Variables

Variable	Dimension	Indicator	Scale	Number of Items	Scoring	References
Cybersecurity Awareness	Understanding of Generative AI & Deepfake	Understanding the concept of AI-based visual manipulation	Likert Scale (1–5)	8	1–5	**[1], [14]**
Cybersecurity Awareness	Cybersecurity Risk Awareness	Awareness of privacy risks and visual identity misuse	Likert Scale (1–5)	8	1–5	**[11], [14]**
Cybersecurity Awareness	Digital Protective Behavior	Content verification behavior and digital visual security practices	Likert Scale (1–5)	8	1–5	**[11], [13]**
Visual Detection Ability	AI-Generated Synthetic Image Detection	Ability to distinguish authentic and AI-generated images	Dichotomous	10	0–10	**[5], [7]**

Validity and reliability testing were conducted through pilot testing involving 30 respondents outside the main sample. Content validity was assessed using expert judgment, while item validity was evaluated using Corrected Item-Total Correlation with a minimum criterion of ≥ 0.30. Reliability testing employed Cronbach's Alpha with a minimum acceptable value of ≥ 0.70. Data were collected online through a digital survey platform, where respondents were first provided with informed consent explaining the study objectives, procedures, and data confidentiality assurances.

Participants completed the awareness questionnaire followed by the image detection test, with an estimated completion time of 15–20 minutes, and the platform was configured to restrict multiple submissions from the same respondent. Data analysis was performed using SPSS through four stages: (1) verification of data completeness; (2) descriptive analysis including mean, standard deviation, and categorization; (3) Kolmogorov–Smirnov normality testing to determine

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

the use of parametric or non-parametric approaches; and (4) Spearman correlation analysis to examine relationships between variables, as well as the Mann–Whitney U test to identify differences based on gender.

DISCUSSION

The findings revealed that students' cybersecurity awareness did not show a significant relationship with their ability to detect AI-generated visual manipulation. This finding indicates a gap between conceptual literacy and practical capability, where understanding the concept of visual manipulation does not directly improve accuracy in identifying synthetic content. These results are consistent with previous studies showing that human ability to detect AI-generated content remains limited, even among individuals with relatively high levels of digital literacy (Groh et al., 2022; Nightingale & Farid, 2022).

The average detection accuracy of 67% places students' performance at a moderate level. Considering that in dichotomous tasks the probability of random guessing reaches 50%, the difference of only 17 percentage points emphasizes that improving cybersecurity literacy should not focus solely on knowledge-based understanding, but also on strengthening practical skills in identifying manipulative content. Previous research similarly emphasized that exposure to synthetic media often exceeds human perceptual detection capacity, particularly when deep learning-based generation techniques are involved (Vaccari & Chadwick, 2020).

The finding of a significant negative correlation between conceptual understanding and protective behavior indicates a possible tendency toward overconfidence, where individuals with higher levels of understanding may reduce their vigilance in real-world practice. This interpretation remains tentative because the overconfidence construct was not directly measured in the present study. However, prior studies in cybersecurity behavior have shown that perceived competence can sometimes reduce precautionary actions, especially in digital risk environments (Hadlington et al., 2023).

From a gender perspective, female students demonstrated higher risk awareness than male students, although no significant difference was found in detection ability. This finding suggests that awareness of risk does not necessarily translate into technical capability in identifying threats, supporting the argument that both dimensions represent distinct constructs that require separate interventions. Similar findings were reported in digital literacy and cybersecurity studies, where risk perception and technical detection skills often develop independently (Guess et al., 2020).

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

As a practical implication, cybersecurity literacy mitigation programs should be designed in the form of simulation-based training that allows students to directly practice identifying synthetic content, accompanied by feedback mechanisms to improve critical evaluation skills. At the institutional level, universities may integrate AI-generative cybersecurity literacy materials into curricula as well as extracurricular activities such as workshops or digital awareness campaigns. This recommendation aligns with recent educational approaches emphasizing experiential learning and digital resilience against AI-driven misinformation (UNESCO, 2023).

Validity and Reliability Testing (Pilot Test, N = 30)

The Corrected Item Total Correlation test indicated that most items met the acceptable criterion of ≥ 0.30. Several items with values slightly below 0.30 were retained to preserve content validity and ensure comprehensive representation of indicators within each multidimensional subdimension [13], [16]. The results of the reliability testing are presented in Table 2.

Table 2. Instrument Reliability Test Results

Dimension	Number of Items	Cronbach's Alpha	Status
Conceptual Understanding of Deepfake	8	0.713	**Reliable**
Cybersecurity Risk Awareness	8	0.739	**Reliable**
Digital Protective Behavior	8	0.711	**Reliable**
Overall Instrument	24	0.836	**Highly Reliable**

Level of Cybersecurity Awareness

A descriptive analysis of 99 respondents showed that the level of awareness fell within the high to very high categories across all dimensions. The Conceptual Understanding dimension achieved a mean score of 4.05 (SD = 0.56) a high category. Risk Awareness (M = 4.48; SD = 0.34) and protective behavior (M = 4.64; SD = 0.30) were both in the very high category. The overall mean of 4.39 (SD = 0.24) indicates a very high level of self-reported awareness. The full results are presented in Table 3.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Table 3. Descriptive Statistics for Cybersecurity Awareness Dimensions

Dimension	Mean	SD	Category
Deepfake Conceptual Understanding	4.05	0.56	**High**
Cybersecurity Risk Awareness	4.48	0.34	**Very High**
Digital Protective Behavior	4.64	0.30	**Very High**
Overall Instrument	4.39	0.24	**Very High**

Visual Detection Ability

The detection test results based on 10 visual stimuli consisting of 5 authentic images and 5 AI-generated synthetic images showed that students' detection ability was at a moderate level. The mean detection score was 6.70 (SD = 1.47), with a minimum score of 1 and a maximum score of 10, resulting in an accuracy rate of 67.0%. Based on the interpretation criteria, this value falls within the 60–79% range, which is classified as a moderate category. Considering that dichotomous tasks provide a 50% probability of random guessing, the 17-percentage-point difference between the actual accuracy and chance level indicates that visual perception ability in identifying AI-generated manipulation remains relatively limited. This finding is consistent with previous studies reported by Bray et al. (2023) and Frank et al. (2024). The results are presented in Table 4.

Table 4. Descriptive Statistics of Detection Scores

Variable	Mean	SD	Minimum Score	Maximum Score	Accuracy (%)
Detection Score	6.70	1.47	1	10	67.0%

Normality Test

The Kolmogorov-Smirnov test showed that all variables had significance values of $p < 0.05$, indicating that the data were not normally distributed. Therefore, non-parametric statistics were used for subsequent analyses. The results are presented in Table 5.

Table 5. Results of the Kolmogorov–Smirnov Normality Test

Variable	Statistic	df	Sig. (p)	Conclusion
Understanding Score	0.170	99	0.006	**Not Normally Distributed**
Risk Awareness Score	0.144	99	0.030	**Not Normally Distributed**

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Protective Behavior Score	0.154	99	0.016	**Not Normally Distributed**
Detection Score	0.299	99	0.000	**Not Normally Distributed**

Spearman Correlation Analysis

The results of the Spearman's rank-order correlation analysis are presented in Table 6. No statistically significant relationships were found between the three dimensions of cybersecurity awareness and actual detection ability (p > .05). However, a statistically significant negative correlation was identified between conceptual understanding and protective behavior Protektif (rs = -0,206, p = 0,041). This finding may indicate the presence of optimism bias or overconfidence, in which individuals with higher theoretical understanding tend to perceive themselves as less vulnerable to cyber threats, thereby reducing their engagement in protective behaviors (Debb & McClellan, 2021; Vismara et al., 2021). This interpretation remains tentative and requires further confirmation through explicit measurement of the overconfidence construct in future studies.

Table 6. Results of Spearman Correlation Analysis (rs)

Variable Relationship	***rs***	***p*-value**	**Conclusion**
Conceptual Understanding – Detection Score	-0.100	0.327	Not Significant
Risk Awareness – Detection Score	0.044	0.667	Not Significant
Protective Behavior – Detection Score	0.038	0.707	Not Significant
Conceptual Understanding – Protective Behavior	-0.206	0.041*	Significant

Mann–Whitney U Test

The results of the Mann–Whitney U test are presented in Table 7. A significant difference was found in the risk awareness dimension based on gender (Mean Rank of females = 56.27 vs. males = 43.60; p = .027). No significant differences were identified in the other dimensions or in detection ability, indicating that gender differences did not affect actual detection performance.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Table 7. Results of the Mann–Whitney U Test

Variable	Mean Rank (Male)	Mean Rank (Female)	U	Z	*p*-value	Conclusion
Conceptual Understanding	45.48	54.43	1003.50	-1.556	0.120	**Not Significant**
Risk Awareness	43.60	56.27	911.50	-2.215	0.027*	**Significant**
Protective Behavior	45.20	54.70	990.00	-1.664	0.096	**Not Significant**
Detection Score	52.31	47.74	1112.00	0.866	0.386	**Not Significant**

CONCLUSION

This study investigated the relationship between cybersecurity awareness and the ability to detect AI-generated synthetic images among students of the Information Systems and Technology Education Study Program at UPI Purwakarta. The findings demonstrate that although students exhibited high levels of cybersecurity awareness across conceptual understanding, risk awareness, and protective behavior dimensions, their actual ability to identify synthetic visual manipulation remained only moderate, with a detection accuracy of 67.0%. These results indicate that theoretical literacy and self-reported awareness do not necessarily translate into effective practical detection skills when individuals are confronted with increasingly sophisticated AI-generated visual content.

The Spearman correlation analysis further confirmed that no significant relationships existed between the awareness dimensions and actual detection performance. This suggests that possessing knowledge regarding cybersecurity and digital threats alone is insufficient to improve visual verification accuracy. Interestingly, a significant negative correlation was identified between conceptual understanding and protective behavior, indicating a potential tendency toward optimism bias or overconfidence among students with higher theoretical knowledge. In addition, the Mann–Whitney U analysis revealed a significant gender difference only in the risk awareness dimension, while no gender-based differences were found in actual detection ability.

Overall, this study highlights an important gap between perceived cybersecurity competence and real-world detection capability. The findings emphasize the urgency of integrating simulation-based learning, visual verification exercises, and AI manipulation detection training into higher

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

education curricula. Future studies are recommended to involve larger and more diverse samples, include explicit measurements of overconfidence constructs, and explore intervention-based approaches to strengthen practical cybersecurity resilience against emerging AI-generated threats.

REFERENCES

Basol, M., Roozenbeek, J., & van der Linden, S. (2021). Good news about bad news: Gamified inoculation boosts confidence and cognitive immunity against fake news. *Journal of Cognition, 3*(1), 2–15.

Badan Pusat Statistik. (2024). *Statistik telekomunikasi Indonesia 2024*. BPS Indonesia.

Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review, 107*(6), 1753–1820.

Citron, D. K., & Chesney, R. (2019). Deepfakes and the new disinformation war. *Foreign Affairs, 98*(1), 147–155.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems, 27*, 2672–2680.

Groh, M., Epstein, Z., Firestone, C., & Picard, R. (2022). Human detection of machine manipulated media. *Proceedings of the National Academy of Sciences, 119*(13), e2117804119.

Groh, M., Epstein, Z., Firestone, C., & Picard, R. (2022). Human detection of machine-manipulated media. Proceedings of the National Academy of Sciences, 119(13), e2117804119.

Guess, A. M., Lerner, M., Lyons, B., Montgomery, J. M., Nyhan, B., Reifler, J., & Sircar, N. (2020). A digital media literacy intervention increases discernment between mainstream and false news in the United States and India. Proceedings of the National Academy of Sciences, 117(27), 15536–15545.

Hadlington, L., Binder, J., & Stanulewicz, N. (2023). The relationship between cybersecurity awareness, online behavior, and susceptibility to cyber risk: Evidence from higher education students. Computers & Security, 126, 103066.

Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? *Business Horizons, 63*(2), 135–146.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289–296.

McGuire, W. J. (1964). Inducing resistance to persuasion: Some contemporary approaches.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License

Advances in Experimental Social Psychology, 1, 191–229.

Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes: A survey. *ACM Computing Surveys, 54*(1), 1–41.

Nightingale, S. J., & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. *Proceedings of the National Academy of Sciences, 119*(8), e2120481119.

Nightingale, S. J., & Farid, H. (2022). AI-synthesized faces are indistinguishable from real faces and more trustworthy. Proceedings of the National Academy of Sciences, 119(8), e2120481119.

Paris, B., & Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. *Data & Society Research Institute*.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42*, 165–176.

Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in Cognitive Sciences, 25*(5), 388–402.

Roozenbeek, J., van der Linden, S., Goldberg, B., Rathje, S., & Lewandowsky, S. (2022). Psychological inoculation improves resilience against misinformation on social media. *Science Advances, 8*(34), eabo2243.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Analyzing trajectories of information security awareness. *Information Technology & People, 28*(2), 327–352.

UNESCO. (2023). Guidance for generative AI in education and research. UNESCO Publishing.

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust in news. *Social Media + Society, 6*(1), 1–13.

Vaccari, C., & Chadwick, A. (2020). Deepfakes and disinformation: Exploring the impact of synthetic political video on deception, uncertainty, and trust. Social Media + Society, 6(1), 1–13.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 39–52.

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82–97.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-Share Alike 4.0 International License