The Eurasia Proceedings of
Educational and Social Sciences (EPESS)
ISSN: 2587-1730

The Eurasia Proceedings of Educational and Social Sciences (EPESS), 2026

Volume 49, Pages 1-8

ICRET 2026: International Conference on Research in Education and Technology

Demographic Differences in IT Security Risk-taking: Implications for Targeted Training and Prevention

Pal Feher-Polgar
Obuda University

Peter Szikora
Obuda University

Abstract: This paper examines the demographic determinants of risk-taking behavior related to IT security, with a particular focus on the role of age and gender. The analysis is based on a modified DOSPERT questionnaire supplemented with an IT security subscale, which allows for statistical control of general risk-taking dimensions. The empirical study involved 772 university students. The results of multivariate regression analyses show that both age and gender have independent and significant explanatory power in the case of IT security risk-taking, even when controlling for perceived benefits, perceived risks, and probability of action. These results suggest that IT security decisions are not solely based on psychological decision-making mechanisms but are also structured by stable demographic characteristics. The study draws practical conclusions for human resource management, IT security training, and targeted education, emphasizing the need to take into account differences between user groups.

Keywords: IT security, Risk-taking, Demographic differences, Security awareness training, Human factors

Introduction

The everyday use of information and communication technologies has become an integral part of the lives of students in higher education, while the widespread use of digital devices has also created new types of risks. A characteristic feature of IT security risks is that their consequences often do not appear immediately and directly, but in a delayed and difficult-to-perceive manner, which makes it difficult to recognize the risks and adapt behavior accordingly. In this unique digital environment, IT security risk-taking cannot be interpreted purely as a technical issue, but rather as a behavioral phenomenon shaped by individual decisions, routines, and background characteristics.

The study of risk-taking is a classic area of decision theory and behavioral science research, where the literature has long emphasized the role of individual differences (Straub & Welpe, 2014). Previous approaches often treated risk attitudes as a uniform, personality-level characteristic, but the emergence of a domain-specific approach has highlighted that risk-taking depends to a large extent on the context in which the decision-making situation arises (Blais & Weber, 2006). The field of IT security is particularly complex in this regard, as it involves technological, psychological, and organizational characteristics that can activate individual behavior patterns in different ways.

The literature has consistently shown that certain demographic factors, particularly gender and age, are associated with systematic differences across a number of risk domains. Men generally show a higher willingness to take risks, while with increasing age, risk-averse behavior often becomes more characteristic. However, these correlations do not appear in the same way in all risk areas, and the specificities of decision-making situations related to digital technologies may modify traditional demographic patterns. Increased

- Selection and peer-review under responsibility of the Organizing Committee of the Conference

technological routine, everyday use of devices, and early socialization into the digital environment can have effects that lead to underestimation or different perceptions of risks (Alghamdi, 2022).

Research on IT security increasingly draws attention to the decisive role of the human factor, emphasizing that technical protection solutions alone are not sufficient to manage digital risks (Keszthelyi, 2015; Szikora & Ali, 2018). However, these approaches typically do not go into detail about the extent to which individual behavior is structured along stable demographic characteristics, especially when we subject general risk-taking propensity to statistical control. As a result, it remains an open question to what extent risk-taking related to IT security can be considered a specific manifestation of general risk attitudes and to what extent it reflects independent, demographic-based differences (van Schaik et al., 2017).

Responding to this gap, the present paper examines the demographic determinants of IT security risk-taking, with a particular focus on the role of age and gender. The aim of the research is to investigate the extent to which these background variables contribute to explaining IT security risk-taking behavior, even when general risk-taking dimensions are statistically controlled for. In this way, the paper contributes to research examining the human factors of IT security and aims to provide an empirical basis for planning targeted educational and preventive interventions among higher education students.

Literature review

Research into risk-taking has a long history in the fields of psychology, economics, and decision theory, and literature initially interpreted risk attitudes primarily as a uniform, personality-level characteristic. These approaches were based on the assumption that individuals have a relatively stable attitude toward risk, regardless of the specific decision-making situation. However, empirical findings have shown over time that risk-taking depends to a significant extent on the decision-making context, which has led to the development of a domain-specific approach. According to this approach, individuals may exhibit different risk patterns in different domains, depending on the type of consequences, uncertainty, and benefits they face (Blais & Weber, 2006).

One of the most widely used tools for empirically measuring domain-specific risk-taking is the Domain-Specific Risk-Taking (DOSPERT) questionnaire, which allows for a structured examination of risk-taking propensity across multiple decision-making dimensions. When using this measurement tool, the literature emphasizes that, in addition to aggregate risk indicators, it is also justified to conduct a controlled analysis of individual background variables, especially demographic characteristics, as these can independently contribute to explaining behavioral differences (Behavioral Science for Policy Lab, n.d.). In this regard, DOSPERT not only serves to measure risk-taking, but also provides a framework in which psychological and demographic factors can be examined separately.

The role of demographic factors in explaining risk-taking is a recurring theme in the literature. Numerous empirical studies have shown that gender differences are particularly pronounced in certain risk domains, where men typically show a higher propensity for risk-taking. These differences are often explained by biological, socialization, or cultural factors, emphasizing the importance of gender role expectations and learning processes (Straub & Welpe, 2014). At the same time, several studies have also pointed out that gender differences may decrease when general risk-taking dimensions and perceived benefits are statistically controlled, suggesting that the effect of gender is partly indirect (Carcelén-García et al., 2023).

The effect of age on risk-taking also presents a complex picture. According to classical decision theory approaches, risk aversion increases with age, which is explained by growing experience and a more serious assessment of potential losses. However, in decision-making situations related to digital technologies, these correlations do not always hold true. The early technological socialization of younger generations and the routine use of IT tools can result in adaptive behavior patterns that may even lead to an underestimation of risks as they age (Nagari & Raharja, 2025). This is particularly relevant in the field of IT security, where risks are often invisible or delayed.

Research into IT security is placing increasing emphasis on the human factor, recognizing that the effectiveness of technical protection solutions depends largely on user behavior. Numerous studies have pointed out that a significant proportion of security incidents are not due to technical errors, but rather to carelessness, rule violations, or risky decisions (Keszthelyi, 2015; Szikora & Ali, 2018). However, these studies typically interpret risks in an organizational or case-specific context and rarely examine the extent to which individual behavioral

differences are related to stable demographic background variables, especially when general risk-taking propensity is controlled for (Patterson & Winston-Proctor, 2019).

Therefore, empirical research on digital risks and IT security behavior still lacks studies that analyze the combined effect of demographic factors and general risk dimensions within a unified measurement framework. Although the role of gender and age has been examined in numerous studies in the general context of risk-taking, controlled empirical testing of these effects in the context of IT security risks remains limited (van Schaik et al., 2017). The present paper contributes to the literature at this point and aims to explore the extent to which age and gender contribute to explaining IT security risk-taking, even when general risk-taking dimensions are statistically controlled for.

Literature Review Research Questions and Hypotheses

When examining risk-taking related to IT security, it remains an open question to what extent individual background characteristics contribute to explaining behavioral differences, especially when general risk-taking propensity is statistically controlled for. Although the role of gender and age in the general context of risk-taking has been confirmed by numerous empirical studies, controlled examination of these effects in the field of IT security remains limited. Due to the specific nature of decision-making situations related to digital technologies, it is unclear whether traditional demographic patterns also apply in this particular domain.

The aim of this study is to empirically examine the relationship between age and gender and IT security risk-taking when the general risk-taking dimensions—perceived benefit, perceived risk, and probability of action—are statistically controlled. Accordingly, the following research question was formulated:

RQ

To what extent do age and gender explain IT security risk-taking, controlling for general risk-taking dimensions?

Based on the literature, it can be assumed that the impact of demographic factors does not disappear completely even when general risk-taking propensity is taken into account, but the direction and strength of these effects may differ from the patterns observed in traditional risk domains. The following hypotheses were formulated to test this empirically:

H1 (Age Hypothesis): Age is positively related to IT security risk-taking, controlling for general risk-taking dimensions.

H2 (Gender Hypothesis): Gender is not significantly related to IT security risk-taking, controlling for general risk-taking dimensions.

The above research question and hypotheses allow us to examine the extent to which IT security risk-taking can be explained by stable demographic background variables and whether these effects remain even when we take into account individuals' general risk-taking propensity. This approach clearly distinguishes the focus of this study from research that primarily examines the structure or psychological mechanisms of decision-making dimensions.

Methodology

The aim of the research was to empirically examine the demographic determinants of risk-taking related to IT security, with particular regard to the role of age and gender, while statistically controlling for general risk-taking dimensions. Data collection was carried out using a quantitative, cross-sectional research design and a self-administered questionnaire. The study was conducted in November 2025 among students at a Hungarian higher education institution. Sampling was convenience-based, and data collection took place in the context of courses related to educational activities. Participation was voluntary and anonymous, and respondents were informed in advance about the purpose of the research and that the data would be used exclusively for research purposes.

The final sample size included 772 individuals. Respondents ranged in age from 17 to 46, with a mean age of 21.44 (SD = 2.65). The gender distribution of the sample reflected the imbalance typical of the higher education student population: 82.8% of participants were male (n = 639), while 17.2% were female (n = 133). Demographic variables were included as explanatory variables in the regression analyses; age as a continuous variable, while gender was included in binary coding (1 = male, 2 = female). This type of coding of the gender variable allowed for a clear interpretation of the regression coefficients, where a positive sign indicated higher values for female respondents in terms of the outcome variable under study.

The measurement tool used in the study was a Hungarian adaptation of the Domain-Specific Risk-Taking (DOSPERT) questionnaire (Blais & Weber, 2006; Radnóti, 2012), which was used to measure general risk-taking propensity. DOSPERT operationalizes risk-taking along three decision dimensions: perceived benefit, perceived risk, and perceived probability of action. In the present study, these dimensions were included solely as control variables in order to isolate the explanatory power of demographic factors from the effect of general risk-taking propensity.

A modified, domain-specific scale was used to measure IT security risk-taking, which initially contained five situational items related to everyday digital device use. The items represented typical IT security risks, such as the unsafe transmission of company data, the use of public networks, or the storage of sensitive information on personal devices. During the empirical analysis, one item was removed from the scale due to low correlation, so IT security risk-taking was ultimately operationalized using a composite indicator consisting of four items. The internal reliability of the scale was moderate (Cronbach's alpha = 0.52), which can be explained by the low number of items and the heterogeneity of the situations, and can be considered acceptable in an exploratory, domain-specific study.

During the data analysis, descriptive statistical analyses were performed as a first step, followed by Pearson correlation analyses to examine the bivariate relationships between the individual variables. Hierarchical multivariate linear regression analysis was used to test the research question and hypotheses. In the first step of the regression model, general risk-taking dimensions were included as control variables, while in the second step, age and gender were included in the model to examine whether these demographic factors have independent explanatory power for IT security.

In the first step of the regression model, general risk-taking dimensions were included as control variables, while in the second step, age and gender were included in the model to examine whether these demographic factors have independent explanatory power in terms of IT security risk-taking. The analyses were performed using IBM SPSS Statistics 25 software.

Results

As a first step in the empirical analysis, descriptive statistics and bivariate correlation analyses were performed to explore the relationship between IT security risk-taking and general risk-taking dimensions and the demographic variables examined. The average composite indicator measuring IT security risk-taking (ICT_Atlag) was 3.36 (SD = 1.05), which falls in the middle range of the 7-point scale and indicates a moderate level of risk-taking.

Based on the results of Pearson's correlation analysis, IT security risk-taking was significantly and moderately positively correlated with perceived benefits ($r = 0.68$; $p < 0.001$) and perceived probability of action ($r = 0.51$; $p < 0.001$), while it showed a weak but significant negative correlation with perceived risk ($r = –0.25$; $p < 0.001$). No significant relationship was found between age and IT security risk-taking at the bivariate level ($r = –0.004$; $p = 0.91$), which supports the need for multivariate analysis. Table 1 summarizes the correlation relationships between the main variables.

Table 1. Pearson correlations between IT security risk-taking and main variables (N = 772)

Variables	1	2	3	4	5
ICT_AVG					
Benefit_AVG	0,676***	–			
Probability_AVG	0,513***	0,760***	–		
Risk_AVG	–0,251***	–0,423***	–0,384***	–	
AGE	–0,004	–0,108**	–0,088*	0,078*	

Note: * p < 0,05; ** p < 0,01; *** p < 0,001

We used hierarchical multivariate linear regression analysis to test the research question and hypotheses. In the first step of the regression model, general risk-taking dimensions (perceived benefit, perceived risk, probability of action) were included as control variables. In this step, the model was significant and explained a significant portion of the variance in the dependent variable. In the second step, demographic variables, age, and gender were included in the model to examine whether these factors had independent explanatory power when controlling general risk dimensions.

The complete regression model showed a statistically significant fit ($F(5, 766) = 137.20$; $p < 0.001$) and explained 47.2% of the variance in the dependent variable ($R^2 = 0.47$; adjusted $R^2 = 0.47$), indicating a strong model fit. Among the control variables, perceived benefit continued to be a strong and significant predictor ($\beta = 0.70$; $p < 0.001$), while the regression coefficients for perceived likelihood of action and perceived risk were not significant in the full model. Among the demographic variables, both age ($\beta = 0.08$; $p = 0.002$) and gender ($\beta = 0.10$; $p < 0.001$) had significant independent explanatory power with regard to IT security risk-taking, even when controlling for general risk dimensions. The detailed results of the regression analysis are presented in Table 2.

Table 2. Multiple linear regression to explain IT security risk-taking (N = 772)

Variables	B	SE	β	t	p
Constant	–1,36	0,41	–	–3,34	0,001
Benefit_AVG	1,12	0,07	0,70	16,82	<0,001
Probability_AVG	0,03	0,06	0,02	0,44	0,661
Risk_AVG	0,06	0,05	0,04	1,29	0,197
AGE	0,03	0,01	0,08	3,05	0,002
Gender (1=M, 2=F)	0,27	0,07	0,10	3,62	<0,001

Table 3 summarizes the empirical evaluation of the hypotheses. Hypothesis H1, which assumed a positive relationship between age and IT security risk-taking while controlling for general risk-taking dimensions, was empirically supported. Although no significant relationship between age and risk-taking was found at the bivariate level, the results of the regression model show that age has independent explanatory power when psychological risk dimensions are taken into account. Hypothesis H2 was also confirmed, as it showed a non-significant relationship with IT security risk-taking even when controlling for general risk-taking dimensions. The positive regression coefficient suggests that female respondents—with control variables at the same level, taking into account the coding of gender (1 = male, 2 = female)—showed higher IT security risk-taking, which deviates from traditional risk-taking patterns and warrants further interpretation.

Table 3. Empirical evaluation of hypotheses

Hypothesis	Description	Test method	Result	Decision
H1	Age is positively correlated with risk-taking related to IT security	Multiple linear regression (control: benefit, probability, risk)	$\beta = 0,08$; $p = 0,002$	Accepted
H2	Gender is significantly related to IT security risk-taking, alongside control over general risk-taking dimensions.	Multiple linear regression (control: benefit, probability, risk)	$\beta = 0,10$; $p < 0,001$	Accepted

Discussion

The aim of this research was to empirically examine the role of age and gender in explaining risk-taking related to IT security when general risk-taking dimensions are statistically controlled. The results show that the effect of demographic factors in this specific risk domain does not disappear even when psychological decision-making dimensions are taken into account, suggesting that IT security risk-taking cannot be interpreted solely as a specific manifestation of general risk attitudes.

It is particularly noteworthy that age did not show a significant relationship with IT security risk-taking at the bivariate level, but appeared as an independent, positive effect in the controlled regression model. This result suggests that the effect of age on IT security decisions is not direct but rather occurs through interaction with other risk dimensions. In other words, age-related behavioral differences only become apparent when we take

into account individuals' general risk-taking propensity, which justifies the use of multivariate, controlled analytical approaches in this research context.

Gender also had an independent explanatory power in terms of IT security risk-taking. Based on the regression results, female respondents showed higher risk-taking at the same level of control variables, which differs from the patterns often observed in traditional risk-taking domains. This deviation may indicate that in the field of IT security, the perception and interpretation of risks is organized according to a different logic than in the case of classic financial or physical risks, even when controlling for general risk-taking dimensions statistically, and may be related to gender-related socialization patterns, which may manifest themselves differently in this digital environment.

It is important to emphasize that although perceived benefits remained a strong explanatory factor in the regression model among the general risk-taking dimensions, the focus of this study was not on the interpretation of these decision-making dimensions. In this context, the results indicate that demographic effects are not only mediated through perceived benefits but also remain after controlling general risk dimensions. This observation confirms the assertion that age and gender can be independent structuring factors in the field of IT security risk-taking.

The results of the study contribute to the literature examining human factors in IT security by providing empirical evidence of the residual effect of demographic background variables in a decision-making domain where risks are often abstract and delayed. The findings suggest that understanding IT security behavior requires more than just focusing on psychological decision-making dimensions; it is also necessary to consider the stable background characteristics that shape the interpretation and management of digital risks.

The limitations of the study include the cross-sectional research design and the use of a student sample, which limit the generalizability of the results. In addition, the moderate internal reliability of the scale used to measure IT security risk-taking warrants caution in interpreting the results. However, these limitations do not diminish the relevance of the results, but rather point to further research directions, particularly with regard to examining demographic effects in longer-term and different populations.

Discussion Conclusions and Implications

The aim of the study was to empirically examine the extent to which age and gender contribute to explaining risk-taking related to IT security when general risk-taking dimensions are statistically controlled. The results show that the effect of demographic background variables in this specific digital risk domain does not disappear even when general risk attitudes are taken into account, suggesting that IT security risk-taking can be interpreted in part as an independent, demographically structured behavioral phenomenon.

Based on controlled regression analyses, both age and gender had insignificant, independent explanatory power with regard to IT security risk-taking. From a theoretical point of view, these results contribute to the literature on domain-specific risk-taking by empirically supporting the residual role of demographic factors in a decision-making environment where risks are often abstract, appear with a delay, and do not fit perfectly into classic risk-taking patterns.

As a practical implication, the results draw attention to the fact that demographic differences should be taken into account when designing educational and prevention programs aimed at IT security awareness, especially when the target group of the interventions consists of young adults. Instead of uniform, "one size fits all" approaches, interventions that reflect different age- and gender-related behavior patterns may be more effective.

The limitations of the paper include the cross-sectional research design and the use of a student sample, which limit the generalizability of the results. A promising direction for future research may be the use of longitudinal studies and the exploration of how demographic effects evolve in different life situations and organizational environments. Overall, this study contributes to a more complex understanding of IT security risk-taking by highlighting the persistent and significant role of demographic factors in digital risk decisions.

Scientific Ethics Declaration

* The authors declare that the scientific ethical and legal responsibility of this article published in EPESS journal belongs to the authors.

Conflict of Interest

* The authors declare that they have no conflicts of interest

Funding

* This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Acknowledgements or Notes

* This article was presented as a poster presentation at the International Conference on Research in Education and Technology (www.icret.net) held in Konya/Türkiye on April 02-05, 2026.

* The authors would like to express their deepest appreciation to the organizers, for their flawless execution and professional dedication. We are grateful for the opportunity to contribute to this event, which stands as a testament to our strong partnership and shared commitment. We thank the committee for their warm hospitality and for fostering such an inspiring professional community.

References

Alghamdi, A. (2022). A systematic review on human factors in cybersecurity. *International Journal of Computer Science and Network Security, 22*(10), 282–290. https://doi.org/10.22937/IJCSNS.2022.22.10.36

Behavioral Science for Policy Lab. (n.d.). *DOSPERT scoring instructions*. Princeton University, Andlinger Center for Energy and the Environment. Retrieved from https://sites.google.com/decisionsciences.columbia.edu/dospert/scoring-instructions

Blais, A.-R., & Weber, E. U. (2006). A domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making, 1*(1), 33–47.

Carcelén-García, S., Díaz-Bustamante Ventisca, M., & Galmes-Cerezo, M. (2023). Young people's perception of the danger of risky online activities: Behaviours, emotions and attitudes associated with their digital vulnerability. *Social Sciences, 12*(3), 164. https://doi.org/10.3390/socsci12030164

Keszthelyi, A. (2015). *Paradigmaváltás – biztonság – emberi tényező*. Taylor: Gazdálkodás- és szervezéstudományi folyóirat, 7(1–2), 406–412. http://acta.bibl.u-szeged.hu/36354/1/vikek_018_019_406-412.pdf

Nagari, S. F., & Raharja, S. (2025). Cyber security awareness, knowledge and behavior of digital banking users in Salatiga. *Asia Pacific Fraud Journal, 10*(1), 15–29.

Nemzeti Média- és Hírközlési Hatóság. (2020, November). *A Nemzeti Média- és Hírközlési Hatóság mobilpiaci jelentése (2015 Q4–2020 Q2)*. Retrieved from https://nmhh.hu/dokumentum/216281/NMHH_mobilpiaci_jelentes_2015Q4_2020Q2.pdf

Patterson, W., & Winston-Proctor, C. E. (2019). *Behavioral cybersecurity: Applications of personality psychology and computer science* (1st ed.). New York, NY: CRC Press. https://doi.org/10.1201/9780429461484

Straub, D., & Welpe, I. (2014). Decision-making under risk: A normative and behavioral perspective. In C. Klüppelberg, D. Straub, & I. Welpe (Eds.), *Risk - A multidisciplinary introduction* (pp. 33–54). Cham: Springer. https://doi.org/10.1007/978-3-319-04486-6_3

Szikora, P., & Ali, B. (2018). Information security in the 21st century – Smart phones in focus. In *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 255–260). IEEE. https://doi.org/10.1109/SISY.2018.8524767

Szikora, P., & Lazányi, K. (2022). *The end of encryption? – The era of quantum computers*. In Security-related advanced technologies in critical infrastructure protection (pp. 61–72). Springer. https://doi.org/10.1007/978-94-024-2155-4_6

Szikora, P., & Lazányi, K. (2022). The end of encryption? – The era of quantum computers. In *Security-related advanced technologies in critical infrastructure protection* (pp. 61–72). Cham: Springer. https://doi.org/10.1007/978-94-024-2174-3_5

van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*, 547–559. https://doi.org/10.1016/j.chb.2017.05.038

Authors Information

Pal Feher-Polgar
Obuda University Keleti Károly Faculty of Business and Management, 1084 Budapest, Tavaszmező str. 17, Budapest, Hungary.
ORCID iD: https://orcid.org/0000-0002-4650-5253
*Contact e-mail: *feherpolgar.pal@kgk.uni-obuda.hu*

Peter Szikora
Obuda University Keleti Károly Faculty of Business and Management, 1084 Budapest, Tavaszmező str. 17, Budapest, Hungary
ORCID iD: https://orcid.org/0000-0001-8680-3880

*Corresponding author(s) contact email

To cite this article:

Feher-Polgar, P. & Szikora, P. (2026). Demographic differences in IT security risk-taking: Implications for targeted training and prevention. *The Eurasia Proceedings of Educational and Social Sciences (EPESS), 49,* 1-8.