

Perceptions of cybersecurity challenges and the need for effective measures

Sanela Ravlić^{a*}, Ivana Unukić^b

^a University of Slavonski Brod, Department of Social Sciences and Humanities, Croatia

^b J. J. Strossmayer University of Osijek, Faculty of Economics and Business in Osijek, Croatia

Article info

Original scientific paper

DOI:

<https://doi.org/10.71159/icemit2523R>

This is an open access paper under the license 

Acknowledgements: This paper presents the results of research conducted as part of the scientific research project under the title “Cyber Festung“, (project code FSTP-OI-22). The project is financed by the European Union and Erste Bank.

Abstract

This paper examines individual perceptions of cybersecurity risks, levels of awareness, and trust in protective measures, with particular attention to generational differences. A sample of 384 respondents from diverse demographics in Croatia completed a structured questionnaire. Descriptive and inferential (ANOVA) analyses were conducted to identify patterns in perceptions across age groups, employment status, and digital experience. The findings reveal a significant age gap, with younger respondents displaying more proactive attitudes but also greater scepticism towards institutional safeguards. The results underscore the urgent need for tailored educational interventions, institutional policy support, and cross-generational mentoring to build a resilient cybersecurity culture.

Keywords: cybersecurity, age gap, Croatia

1. Introduction

In the modern world, particularly in the digital era, cybersecurity is not only a technical issue but also a social and psychological one. Technical solutions such as anti-virus software, firewalls, and encryption are often available, but their effectiveness depends on whether people use or ignore them. Previous research clearly shows that risk perceptions, the degree of trust in institutions, and end-user habits significantly influence the actual level of security (Petruzzini et al., 2021; Al-Hawawreh et al., 2023).

A particular challenge is the generation gap (“age gap”), as younger generations, already integrated into the digital world, have different attitudes, expectations, and practices regarding cybersecurity compared to older generations. This can lead to uneven resistance and weak links in the protection chain. Dhungana et al. (2023) state that students and teachers have different levels of awareness of cyber threats, as well as different approaches to protection, further confirming that demographic variables such as age and experience significantly shape perceptions and behaviour in security.

The objectives of this paper are: (1) to analyse threat perceptions and awareness levels in a sample of 384 respondents; (2) to examine the relationship between demographic factors, especially age group, and these perceptions; and (3) to formulate recommendations for educational and institutional measures aimed at closing the “age gap” in the field of cybersecurity. The recent review of hospitality food waste (Filimonau et al., 2021b; Filimonau et al., 2023; Papargyropoulou et al., 2023; Wang et al., 2017; Kattiyapornpong et al., 2023; Bharucha, 2018; Vizzoto et al., 2020) emphasises the complexity of the hospitality sector impacting distinct food waste management practices. Theoretically, Food Waste Hierarchy Model is applied widely in waste management, but only a few studies in hospitality food waste management (Sirijuntrapun et al., 2022). Therefore, one of the tasks of the research is to compare the results with theoretical model and as well as the application in practice through a corporate social responsibility.

2. Previous research – literature review

Al-Hawawreh et al. (2023) point out that the perception of threats on the Internet is often a function of digital literacy; those who better understand technology are better able to assess dangers. Okoye I et al. (2024) states that sensitive

*Corresponding author

E-mail address: sravlic@unisb.hr

domains such as finance have high security requirements, but users often overestimate the protection provided to them (e.g. banking measures).

Chaudhary et al. (2020) discuss that younger generations (Generation Z and Millennials) possess greater technical competence, but also a greater tendency towards scepticism of institutions and therefore less trust in national or corporate control measures. Other works in the literature on digital literacy confirm that older generations (e.g. those aged 50 and above) use advanced security measures less frequently and tend to rely on "what the system does itself". Stanfield (2024) points out that as mobile device usage increases, so do threats, and that user habits and behaviours on mobile platforms significantly influence risk exposure. Furthermore, Gomez and Shandler (2024) state that the closer a person is (spatially, socially, or psychologically) to a risk, the greater the perception of threat and the lower the trust in institutions, indicating that experience (or perception of exposure) shapes attitudes towards regulation and protective policies.

Several authors point out that technological tools alone are not sufficient, and that education and continuous awareness are key. Many studies show that training systems, simulations, and mentoring programmes strengthen users' cognitive capacities (encouraging proactive behaviour) and reduce human error in the security domain. Gerdenitsch et al. (2023) find that security knowledge, perception of risk severity and susceptibility, and working conditions significantly influence employee security behaviour, which implies that educational programmes must take into account not only content, but also psychological and organisational factors. A multidisciplinary approach that combines technical, organisational, and educational components is also considered best practice (Al-Hawawreh et al., 2023; Chaudhary et al., 2020).

Based on the above, the authors propose three hypotheses:

H1: There is a statistically significant difference in attitudes towards readiness for additional education and increasing knowledge and skills in cybersecurity with respect to the status of the respondents.

H2: There is a statistically significant difference in attitudes towards readiness to allocate financial resources for additional education in cybersecurity with respect to the status of the respondents.

H3: There is a statistically significant difference in attitudes towards readiness to allocate financial resources for additional education with respect to the age of the respondents.

A recent literature review also shows a wide range of approaches to risk perception and security behaviour: from generational studies (e.g. Dhungana et al., 2023), which show differences in awareness and learning habits, to studies on mobile threats (Stanfield, 2024), and analyses on how working conditions and autonomy affect security. This reflects a trend in which technical, educational, and social aspects are integrated for a more comprehensive understanding of cybersecurity.

3. Methodology

The research presented in this paper was conducted in the first half of 2025 as part of the Cyber Festung project, which focuses on strengthening cybersecurity awareness, resilience, and education among individuals and organisations. The survey was distributed to both legal entities and individual respondents across Croatia, with this analysis focusing exclusively on data collected from individuals. A total of 384 valid responses were obtained from individuals. Participants completed a questionnaire consisting of several demographic questions and seventy thematic questions addressing various aspects of cybersecurity perceptions, behaviours, and challenges. To answer the questions, respondents were offered a 5-point Likert scale, which, for the purposes of this paper (Table 6 and Table 8), was interpreted as three levels: 1 – I agree, 2 – I neither agree nor disagree, 3 – I disagree. The entire survey was compiled from various studies, with the work of Ricci et al. (2019) being particularly significant for this research paper.

For this analysis, three selected questions were included, chosen for their relevance to understanding perceptions of cybersecurity challenges and for examining the relationship between demographic variables (age, status) and perceptions of cybersecurity. The collected data were analysed using IBM SPSS Statistics 23. Descriptive statistics were used to summarise the responses, while inferential analyses, specifically Analysis of Variance (ANOVA), were applied to examine potential associations and differences between demographic variables and responses to the selected cybersecurity-related items.

Looking at differences by gender (Table 1), out of 384 respondents, 136 were men (35.4%) and 243 were women (63.3%), while 1.3% did not wish to state their gender.

Table 1. Gender structure of respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
Male	136	35.4	35.4	35.4
Female	243	63.3	63.3	98.7
Don't want to answer	5	1.3	1.3	100.0
Total	384	100.0	100.0	

Source: Author's calculation based on SPSS 23.0

This (Table 1) may reflect women's greater interest in participating in digital habits research or their greater availability at the time of the survey. However, it is possible that this distribution is influenced by a bias towards perceptions of security issues, as the literature sometimes suggests that women tend to be more protective in digital contexts (Anwar et al., 2017), which may affect interpretation.

Regarding the status of the respondents, the majority are students (172, or 44.8%) and pupils (155, or 40.4%). A smaller percentage (14.1%) are employed. One per cent of the respondents are retired, unemployed, or classified as other.

Table 2. Employment status of respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
Highschool students	155	40.4	40.4	40.4
University students	172	44.8	44.8	85.2
Employed	54	14.1	14.1	99.2
Unemployed	1	0.3	0.3	99.5
Retired	1	0.3	0.3	99.7
Don't want to answer	1	0.3	0.3	100.0
Total	384	100.0	100.0	

Source: Author's calculation based on SPSS 23.0

The differences in Table 2 are important because students and employees may have different levels of exposure to digital risks and varying experience with technology. Students may be more technologically active, while employees may have experience with institutional systems and security in the workplace. All respondents were asked whether they had ever participated in a cybersecurity workshop. As expected, 65.6% (252 respondents) had never participated in a cybersecurity workshop (Table 3).

Table 3. Attendance of cybersecurity workshops of respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
No	252	65.6	65.6	65.6
Yes	132	34.4	34.4	100.0
Total	384	100.0	100.0	

Source: Author's calculation based on SPSS 23.0

The majority of respondents access the internet via a smartphone (88.8%), while 10.6% use a desktop computer or laptop. A further 0.5% indicated that they access the internet in other ways.

Table 4. Internet access methods of respondents

	Frequency	Percent	Valid Percent	Cumulative Percent
Table Computer	19	4.9	4.9	4.9
Laptop	22	5.7	5.7	10.7
Smartphone	341	88.8	88.8	99.5
Other	2	0.5	0.5	100.0
Total	384	100.0	100.0	

Source: Author's calculation based on SPSS 23.0

According to Table 4, almost all respondents (88.8%) access the Internet via a smartphone, confirming the trend of mobile dominance in the digital environment. Laptops and desktops together account for about 10.6% of access, while alternative methods are negligible (0.5%). The results suggest that most security risks and educational campaigns should focus on mobile platforms, as they are the main channel for digital communication and exposure to cyber threats. They also indicate that respondents' digital behaviour predominantly occurs via mobile devices, supporting recent research that highlights the importance of mobile security and user behaviour (e.g. Odeyemi, 2024; Chaudhary et al., 2020).

Table 5. Age structure of respondents

Age			
N		Valid	384
		Missing	0
Mean			21.43
Median			19.00
Mode			17
Std. Deviation			7.066
Range			41

Source: Author's calculation based on SPSS 23.0

According to Table 5, the average age of the respondents is 21.4 years, indicating that the sample consists mainly of young people, primarily students and pupils. The median age of 19 years and the mode of 17 confirm that the largest group is in

early adulthood. The range of 41 years shows that older respondents also participated in the study, allowing for the analysis of generational differences, although the predominance of younger respondents affects the generalisability of the results. Table 5 demonstrates that young respondents are dominant in the sample, which implies a higher degree of digital exposure and skills, but also potentially greater scepticism towards institutional security measures, as confirmed by the findings of Al-Hawawreh et al. (2023).

4. Results and discussion

This section presents the main findings of the research on perceptions of cybersecurity challenges and the need for effective measures among individual respondents. The analysis is based on the responses of 384 participants to two selected survey questions, covering awareness of cybersecurity risks, personal practices related to digital security, and attitudes towards institutional and individual responsibility in cybersecurity protection. The results are first presented using descriptive statistics to outline general trends and distributions across the sample, followed by inferential analyses aimed at identifying statistically significant relationships and differences between demographic characteristics and respondents' cybersecurity perceptions. These findings provide a foundation for understanding how demographic factors may influence awareness and behaviour in the context of cybersecurity challenges.

Table 6. Descriptives table for the first two hypotheses

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
In the next 6 months, I plan to further educate myself and increase my knowledge and skills about my cybersecurity.	1	122	2.37	0.815	0.074	2.22	2.51	1	3
	2	154	2.51	0.760	0.061	2.39	2.63	1	3
	3	48	2.71	0.582	0.084	2.54	2.88	1	3
	Total	324	2.49	0.765	0.042	2.40	2.57	1	3
I am willing to allocate financial resources to further educate myself about cybersecurity.	1	134	1.87	0.891	0.077	1.71	2.02	1	3
	2	153	2.02	0.892	0.072	1.88	2.16	1	3
	3	51	2.39	0.777	0.109	2.17	2.61	1	3
	Total	338	2.01	0.890	0.048	1.92	2.11	1	3

Source: Author's calculation based on SPSS 23.0

Table 7. ANOVA table for the first two hypotheses

		Sum of Squares	df	Mean Square	F	Sig.
In the next 6 months, I plan to further educate myself and increase my knowledge and skills about my cybersecurity.	Between Groups	4.158	2	2.079	3.612	0.028
	Within Groups	184.792	321	.576		
	Total	188.951	323			
I am willing to allocate financial resources to further educate myself about cybersecurity.	Between Groups	10.246	2	5.123	6.686	0.001
	Within Groups	256.680	335	0.766		
	Total	266.926	337			

Source: Author's calculation based on SPSS 23.0

Tables 6 and 7 describe the analysis of the first two hypotheses. Based on the results of a one-way analysis of variance for independent samples, it is concluded that respondents differ statistically significantly in their attitudes towards willingness to undertake additional training and increase their knowledge and skills in cybersecurity with regard to their status ($F(2, 321) = 3.612, p < 0.05$). The observed difference is not considered random, but the results do not indicate which groups differ from each other.

Based on the results of a one-way analysis of variance for independent samples, it is concluded that respondents differ statistically significantly in their attitudes towards willingness to allocate financial resources for additional training in cybersecurity with regard to their status ($F(2, 335) = 6.686, p < 0.05$). The observed difference is not considered random, but the results do not indicate which groups differ from each other.

Tables 8 and 9 describe the analysis of the last hypothesis. Based on the results of a one-way analysis of variance for independent samples, it is concluded that respondents differ statistically significantly in their attitudes towards the willingness to allocate financial resources for additional education with respect to age ($F(2, 337) = 5.797, p < 0.05$). The observed difference is not considered random, but the results do not indicate which specific groups differ from each other.

Table 8. Descriptives table for the third hypothesis

		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
I am willing to allocate financial resources to further educate myself about cybersecurity.	1	134	1.87	0.891	0.077	1.71	2.02	1	3
	2	153	2.02	0.892	0.072	1.88	2.16	1	3
	3	51	2.39	0.777	0.109	2.17	2.61	1	3
	Total	338	2.01	0.890	0.048	1.92	2.11	1	3

Source: Author's calculation based on SPSS 23.0

Table 9. ANOVA table for the third hypothesis

		Sum of Squares	df	Mean Square	F	Sig.
I am willing to allocate financial resources to further educate myself about cybersecurity.	Between Groups	8.943	2	4.471	5.797	0.003
	Within Groups	259.913	337	0.771		
	Total	268.856	339			

Source: Author's calculation based on SPSS 23.0

The results indicate a pronounced age gap in the perception of cybersecurity. Although younger age groups (e.g. 18–25) demonstrate greater awareness and readiness to apply protective measures, they also exhibit greater scepticism towards institutional solutions (e.g. measures implemented by IT departments or government regulations). This suggests a paradox: a better understanding of risk does not necessarily lead to greater trust in formal protection systems.

All three hypotheses were confirmed by these tests.

This pattern is supported in the literature: the paper "Emerging challenges in cybersecurity and resilience" (Chaudhary et al., 2020) states that younger generations demand transparency, participation, and a sense of "having control" over their digital security, which often conflicts with "top-down" institutional approaches. In contrast, older groups (50+) may have less technical awareness and overestimate the protection provided by institutions, but often display a higher degree of trust, as they are accustomed to the model "the institution knows" and "the state or work environment takes care of me." This is reinforced by lower digital literacy, resulting in lower threat assessments but fewer demands for additional protections.

This dual effect: high awareness but greater scepticism among young people; lower perception but higher trust among older people; implies that policy and education must not be universal. It is necessary to implement:

- Segmented education and communication: approaches tailored to each generation;
- Intergenerational mentoring programmes: enabling older and younger people to share experiences and suggestions (which can reduce the gap);
- Participatory institutions: involving users in the design of security protocols and ensuring transparency of the process;
- Practical training and simulations that incorporate user perspectives (e.g. "hackathon" simulations, gamification).

Ultimately, the results suggest that technical solutions, without consideration of psychological and demographic differences, will not achieve maximum effectiveness.

5. Conclusion

Findings presented in this paper indicate that threat perceptions and trust in protective measures are not homogeneous categories; the existence of a generational gap is crucial for understanding how to build effective security strategies. Young respondents demonstrate high awareness but also greater scepticism towards institutional measures, while older respondents display less technical sensitivity but greater trust.

Recommendations to improve trust in the field of cybersecurity include:

- Targeted educational campaigns for different age groups, with varied communication styles (videos, workshops, interactive simulations).
- Intergenerational mentoring, introducing programmes in schools, colleges, and organisations where younger and older people collaborate on security projects.
- Participatory policy and security protocol development, involving users in system design (e.g. surveys, focus groups).

- Feedback and transparency systems, providing users with insight into the measures organisations are implementing and the results of evaluations.
- Ongoing monitoring and evaluation, conducting longitudinal studies and tracking changes over time.
- If implemented, these measures can help close the “age gap” in cybersecurity and build a more coherent, resilient digital community.

Despite these valuable insights, this research has several limitations that should be considered when interpreting the results. First, the sample size and structure (although 384 respondents is a respectable number): the sample is not representative of the entire Croatian population. The research is dominated by students and younger people, which may bias the perception of digital competence and awareness of risks. This reduces the possibility of generalising the results to older and less digitally literate groups. Second, the research is based on self-assessments, meaning that the responses may be subjective and influenced by social desirability: respondents may report a higher level of awareness and responsibility than they actually demonstrate in practice. Third, the research has a cross-sectional character: the data were collected at a single point in time, so it is not possible to observe changes in behaviour and perceptions over time. Fourth, the focus was on individual perceptions and basic demographic variables (age, gender, status), while organisational, cultural, and institutional factors were not analysed in detail. This omits deeper insights into how organisational context (e.g. corporate, academic, or state policy) influences actual security practices.

To improve understanding of this issue, future research should:

- Broaden the sample to include respondents from different age, educational, and geographical groups to ensure representativeness and better understanding of differences between urban and rural areas.
- Introduce a longitudinal approach; by monitoring changes in perceptions and behaviours over time, it is possible to see how educational campaigns or new security incidents affect awareness and behaviour.
- Combine quantitative and qualitative methods; for example, focus groups and interviews can reveal deeper reasons for scepticism towards institutions, personal motivations, and emotional reactions to risks.
- Analyse the institutional and organisational context; explore the role of employers, educational institutions, and government bodies in building a security culture.
- Compare international patterns; including comparative samples from other countries would allow the identification of cultural and structural differences in the perception of cyber threats and the effectiveness of educational measures.

In this way, a holistic cybersecurity paradigm could be developed, encompassing technical, psychological, educational, and social dimensions—with particular emphasis on moving from reactive to proactive approaches and closing the generational gap in digital security.

References

- Al-Hawawreh, M., Aljuhani, A., & Jararweh, Y. (2023). Chatgpt for cybersecurity: practical applications, challenges, and future directions. *Cluster Computing*, 26(6), 3421-3436. <https://doi.org/10.1007/s10586-023-04124-5>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437-443. <http://dx.doi.org/10.1016/j.chb.2016.12.040>
- Chaudhary, H., Detroja, A., Prajapati, P., & Shah, P. (2020, December). A review of various challenges in cybersecurity using artificial intelligence. In *2020 3rd international conference on intelligent sustainable systems (ICISS)* (pp. 829-836). IEEE. <https://doi.org/10.1109/ICISS49785.2020.9316003>
- Dhungana, R. K., Gurung Dr, L., & Poudyal, H. (2023). Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal. *Journal of Cybersecurity Education, Research and Practice*, 2023(2), 5. <https://doi.org/10.32727/8.2023.17>
- Gerdenitsch, C., Wurhofer, D., & Tscheligi, M. (2023). Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees' security behavior. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 17(4). <https://doi.org/10.5817/CP2023-4-7>
- Gomez, M. A., & Shandler, R. (2024). Trust at risk: The effect of proximity to cyberattacks. *Journal of Global Security Studies*, 9(2), ogae002. <https://doi.org/10.1093/jogss/ogae002>
- Okoye, C. C., Nwankwo, E. E., Usman, F. O., Mhlango, N. Z., Odeyemi, O., & Ike, C. U. (2024). Securing financial data storage: A review of cybersecurity challenges and solutions. *International Journal of Science and Research Archive*, 11(1), 1968-1983. <https://doi.org/10.30574/ijrsra.2024.11.1.0267>
- Ricci, J., Breiting, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1), 231-249. <http://dx.doi.org/10.1007/s10639-018-9765-8>
- Stanfield, M. (2024). Mobile Technologies at Risk: A Literature Review on the Evolving Challenges and Solutions in Mobile Technology Security. *Buletin Stiintific*, 29(1). <https://doi.org/10.2478/bsaft-2024-0016>