Medij. istraž. (god. 30, br. 2) 2024. (129-52)
IZVORNI ZNANSTVENI RAD
DOI: 10.22572/mi.30.2.6
Primljeno: srpanj, 2024.

The Impact of Age and Education on Cyber Security in Digital Banking

Manuela Bukovec*
Krunoslav Antoliš**

ABSTRACT

Cybersecurity is the foundation for preserving confidentiality and integrity in the modern digital age. It is crucial for the security of individuals, organizations, and society. This paper is based on these premises, exploring the impact of demographic factors on user perceptions and behaviors regarding cybersecurity in digital banking. The study draws on the socio-technical systems theory, which examines the relationships between social and technical elements within technology usage. The research was conducted through an online survey distributed via posts on social networks such as Facebook, LinkedIn, and Twitter and by emailing the survey to target groups currently engaged in secondary or higher education or already employed. The study involved 212 respondents divided into six age groups. The sample (n=212) was achieved with 100% response quality and a standard deviation of 0%. The research aimed to understand how demographic characteristics, particularly age, influence interactions with digital banking technology and cybersecurity practices. Using multiple regression analysis, two hypotheses were tested hypothesis 1: Older users (aged 45 and above) demonstrate a higher level of caution in online payments compared to younger users (aged up to 44) was rejected, and hypothesis 2: A higher level of education positively influences users' understanding of security

*Manuela Bukovec, PhD student, Alma Mater Europae, mag. oec., mbukovec1309@gmail.com, 00385 (0) 91 450 1129

** Krunoslav Antoliš, PhD, Associate Professor, Police academy "First Croatian Police Officer", Ministry of Internal Affairs, Republic of Croatia, antolisk@yahoo.co.uk, 00385 (0) 91 344 4853

when making online payments with bank cards confirmed. The results indicate that education is a significant predictor of a sense of security, with users having higher levels of education reporting a greater sense of security during online payments. Age and employment status did not prove to be statistically significant factors in explaining users' sense of security within this sample. However, age showed a negative effect, suggesting that older users feel less secure.

*Keywords: Cybercrime, Cybersecurity, Digital Banking, Cyber Fraud, Online Payments*t

Introduction to the field of research

Today, cyber security represents an important factor in the business of all companies, which is based to a significant extent on the constant raising of awareness and knowledge about information, related technologies, adopting cyber security measures, initiating innovations and creating a competitive advantage (Ghelani, 2022; Cartwright et al., 2023: 103288).

The forecasting of information trends related to the most popular cyberattacks, viewed as consequences of cybercrime occurring on the Internet, are topics researched by many authors around the whole world (Kuzior et al., 2022: 613; Katterbauer et al., 2022: 56-61). The profession, criminologists and cybercrime prevention experts, recognize the importance of geographical areas that are more suitable for criminal activities as well as the role that managers of individual locations can play in order to prevent crime as effectively as possible. A large number of works created in the last few decades highlight the tendency to concentrate crime in a number of geographical areas, especially in areas where local governance is weaker or even completely absent (Back and Guerette, 2021: 427-451). Cybercrime ravages the global economy, national security, social stability, and individual interests, and studies show that cybercrime is closely related to socioeconomic development, and that their effects on it differ depending on the level of income (Chen et al., 2023: 1-10).

Today, technology, especially information and telecommunications, controls more and more aspects of life, and the digitization of society ensures the speed of information flow, the reduction of distance and response time to a request or need, deve-

loping a highly digitized sector of goods and services. Digitally delivered products and services, distance learning, online use of bank cards, electronic payments and other digital services intensify cash flows, allowing capital to move to all corners of the world in an instant. All this leads to changes in business, whereby management is forced to adapt to the stresses of globalization and diversification, thereby changing social relations (Hellvig et al., 2020).

The revolutionary development of information technologies (IT) has led to a significant growth in the number of Internet users, which consequently implies serious security risks. Intending to reduce these risks, scientists are investigating many factors and their relationships, such as the association of age with the frequency of Internet use (Adams et al., 2022: 45-62; Furthermore, the theoretical paradigm employed by Mitall and Ilavarasan in their research is also based on the idea that demographic characteristics such as age, education, work experience, and academic discipline significantly influence users' behavior and perceptions related to cybersecurity, suggesting that different demographic groups may differ in their responses due to variations in professional experience, educational background, and cultural context, indicating the need to develop specific interventions that will enhance security behavior within these groups (Mittal & Ilavarasan, 2019: 667-676). To test and expand the results of these works and theoretical premises, especially for Croatian citizens, arises the research question of this study: *How does the age and education of users in Croatia affect their level of caution and sence of security when making online payments in digital banking?*

Literature review in the field of research

Digital transformation of business

The traditional banking sector, known as "fintech," leverages financial technology and telecommunications to provide client-focused services. The evolution of digital banking within established institutions is on the rise, with studies indicating that banking infrastructures need to effectively integrate data sharing, connectivity, stability, cybersecurity, and standardized APIs to protect data and ensure user privacy (Wewege and Thomsett, 2020: 15-56). Cloud computing, a key player in this technological shift, is being scrutinized for its implementation and associated security concerns, especially within the banking sector (Vinoth et al., 2022: 2172-2175). A significant aspect of digital banking is the transition of clients from physical branches to digital platforms, which relies on factors such as effective communication in branches, the digital transformation of services, client-focused initiatives, and the evolving role of branch personnel (Kaur et al., 2021: 107-121).

Traditional banks are increasingly pressured by stakeholders to embrace new technologies while maintaining robust data security. Customer trust remains critical, as a bank's reputation directly influences its success in attracting and retaining clients. This complexity makes decisions about the secure integration of artificial intelligence (AI), digital transformation, and cybersecurity challenging, necessitating a support model that combines cognitive mapping with laboratory testing for decision-making (Rodrigues et al., 2022: 101616). Researchers are also exploring the role of AI in promoting digital financial inclusion, focusing on risk management, information asymmetry, customer support, fraud detection, and cybersecurity. Consequently, financial and non-financial institutions, along with governments, must adopt AI tools to help vulnerable populations engage in the formal financial market with minimal obstacles and maximum benefits (Mhlanga, 2020: 45).

Digital transformation in banking encompasses both internal and external changes. Key to these changes is strategic planning for information systems, alignment between business and service innovation strategies, and leveraging technology to enhance business value. Training programs aimed at improving employees' technological skills, along with reward policies and career development opportunities, are essential (Kitsios et al., 2021: 204; Diener and Špaček, 2021: 2023). While banks' business models still reflect traditional banking theory, there is a growing influence of innovative technologies on financial intermediation. However, client trust remains central, and while liquidity transformation continues to be crucial, the landscape of banking and financial services is evolving rapidly (Broby, 2021: 47).

Research in Russia suggests that legal frameworks for the digitalization of the banking system should be guided by strategic planning documents aimed at promoting sustainable development. However, the concept of financial sustainability is currently debated and remains vague, complicating a comprehensive evaluation of the effectiveness of Russia's banking digital transformation within a sustainable development context. The rapid pace of technological advancement demands timely creation of strategic development documents, comprehensive legal regulations, and the establishment of new mechanisms for implementing state authority (Tsindeliani et al., 2022: 165-180).

Studies indicate a notable increase in the adoption of digital payments and banking services in Gulf countries, revealing challenges such as security concerns and a lack of financial literacy among certain demographic groups. These issues underscore the need for improved security in digital transactions, enhanced financial literacy, and the development of user-friendly solutions (Alkhowaiter, 2020: 102102). Research also shows that digital transformation has positively impacted the success of Vietnamese banks, with effectiveness varying by bank size (Do et al., 2022: 21).

Cyber attacks on banks

Financial institutions play a vital role in the global economy, providing essential services such as liquidity, money supply, loans, savings, deposits, payments, and settlements. However, the frequency and complexity of cyberattacks are on the rise, presenting a serious threat to both the financial system and the broader economy. Blockchain technology could significantly improve cybersecurity in the financial sector by offering built-in protection against such attacks. To effectively tackle this issue, a comprehensive approach is required, which includes clearer delineation of stakeholder responsibilities, international collaboration, minimizing fragmentation, and standardizing regulations to address cross-border crime (Gulyás and Kiss 2023; 84-90; Manoj 2021: 1332-1339).

There is a consensus among researchers regarding the increasing occurrence, severity, and sophistication of cyberattacks on financial institutions. Notably, most of these incidents remain unreported, highlighting the need for financial entities to implement a comprehensive risk management strategy to counter this emerging threat (Camillo 2017: 196-200). Studies suggest that discretionary loan loss reserves can indicate potential cyberattacks, and post-attack, banks tend to reduce their engagement in earnings manipulation. Furthermore, larger banks are more susceptible to these cyber threats (Jin et al. 2023: 103705). The banking sector has seen a rise in cybercrime over the years, with 50% of incidents linked to ATMs, debit cards, and online banking. Compared to other sectors, banks face cyberattacks more frequently, and the main objective of cybersecurity in digital banking is to safeguard digital transactions (Kumar 2023: 43-52).

Advancements in information technology have provided criminals with new avenues to perpetrate cybercrime, using increasingly advanced methods. The surge in cyberattacks is alarming, as they disrupt crucial banking operations and result in significant financial losses. To combat cybercrime and enhance security, financial institutions are focusing on integrating artificial intelligence and other cybersecurity measures to improve customer experiences and streamline banking processes (Hasan and Al-Ramadan 2021: 2312-2323; Creado and Ramteke 2020: 771-780). In today's world, the significance of the internet and computer systems is well acknowledged, offering substantial benefits to society. However, some individuals exploit these advancements for illicit purposes. For instance, cybercrime in India is on the rise for various reasons, complicating the pursuit of cybercriminals. Research indicates an increase in fraud cases, predominantly affecting individuals aged 20 to 29, especially children and women. Awareness initiatives are essential to prevent cybercrime both in India and globally (Datta et al. 2020: 267-275).

Cyber security of the banking sector

Banks serve as the financial foundation of a state and its economy. To effectively combat cyber threats, it is crucial for banks to evolve beyond traditional banking practices, collaborating as a unified entity while embracing new technologies and perspectives (Stanikzai and Shah 2021: 1-4).

In the coming years, cybersecurity, data regulation, and sustainability will be vital components of digital transformation. Banking and financial systems must develop effective tools for sustainable development, and the successful implementation of Information and Communications Technology (ICT) in environmentally-friendly initiatives relies on leveraging the full potential of these technologies through intelligent, informative, and innovative solutions (Sulich et al. 2021: 20-28). However, the rapid advancement of smartphones and applications can lead to reliability issues (Panja et al. 2013: 397-403). Research indicates that blockchain technology should be effectively integrated into various aspects of cybersecurity and accounting, including auditing and general accounting practices (Demirkan et al. 2020: 189-208).

The effectiveness of cybersecurity measures is significantly influenced by the knowledge and skills of banking sector employees responsible for implementing them. Studies reveal a considerable skills gap among employees concerning cyber threats, primarily due to a lack of basic technical skills needed to respond to various cyberattacks. Additionally, communication skills are often lacking. To address this, Al-Alawi and Al-Bassam's research enhances understanding of cybersecurity and its significance for banking institutions, providing banks with valuable insights to improve employee skills in identifying cyber threats (Al-Alawi and Al-Bassam 2020: 1523-1536).

Biometric authentication is gaining traction as a method for protecting cyberspace, benefiting not only the private and public sectors but also consumer electronics and corporate security systems. This approach verifies individuals based on their physical attributes and behavioral traits, making it one of the most reliable and effective methods for identity verification (Khan et al. 2023).

As digitization in banking increases, cybercriminals are becoming more active, making IT an essential backbone of the digital banking framework. Digital banking faces various cyber threats, including phishing, hacking, counterfeiting, and fraud. By employing robust authentication, identification, and verification techniques, these attacks can be effectively mitigated (Kumar 2023: 43-52).

Cybersecurity in the Republic of Croatia

In Croatia, as in the rest of the world, banks face numerous challenges in protecting their customers' data and ensuring the integrity of financial transactions. These challenges become even more complex due to the increased use of digital services, which makes users potential targets of cyberattacks.

Cybersecurity is based on a wide range of practices, tools, and concepts that are closely related to technology. In his work, Galinec explains the concept of "cybersecurity" and describes the relationships between cybersecurity, information security, technological security, IT security, and other related disciplines and practices such as cyber defense, and their implementation in alignment with planned or existing national cybersecurity strategies. In a case study, he also presents and elaborates on an example of the National Cybersecurity Strategy of the Republic of Croatia and the Action Plan, where the primary goal is to identify organizational problems in implementation and expand the understanding of the importance of this issue in society. He concludes that the results of cybersecurity education programs implemented in the Republic of Croatia are questionable. He believes that the development of cybersecurity within the Strategy and Action Plan should serve as a framework for the development of all national educational programs in this area, and that a curricular reform and enhancement of all types and levels of education in the field of cybersecurity and defense in the Republic of Croatia is necessary (Galinec et al. 2017: 273-286).

While many European countries recognized cybersecurity as crucial during the COVID-19 pandemic, Croatia remained completely silent on this issue, leaving companies to find their own ways to respond to the increased cyber threats. Each company was responsible for implementing security controls for remote access. During this period, there were no guidelines or recommendations from the Croatian Government and cybersecurity regulators, leading to the conclusion that cybersecurity awareness should grow proportionally with cybersecurity challenges and that Croatia needs to invest more effort in this segment (Škiljić 2020: 51-61).

In professional police work, the ability to recognize false information is crucial. Critical thinking, the use of fact-checking tools, and education about different disinformation techniques are important. All these measures and procedures help maintain the integrity and effectiveness of police work. Addressing the issue of disinformation in the modern digital age is extremely important and opens up space for further research regarding the selection of the most appropriate approaches and teaching methods (Antoliš 2024: 71-83).

Cyber forensics and education

Cyber forensics is also becoming increasingly of interest to scientists, and its primary task, which involves the identification, collection, analysis, and preservation of digital evidence, represents crucial support in the processes of investigating cybercrime. Key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and internet sexual crime, cyberbullying and stalking, cyberterrorism and extremism, digital forensic investigations and their legal context, as well as cybercrime policy, are covered in the book by a group of authors titled "Cybercrime and Digital Forensics: An Introduction," which is an essential read for courses on cybercrime, cyber deviance, digital forensics, cybercrime investigation, and the sociology of technology (Holt et al. 2022).

With the growth in the number of computers and the use of internet space, the demands for digital forensics in the field of data storage and processing are also increasing. Automation is highly desirable in this field, but it is not easily accessible because unstructured forensic data and the lack of defined semantics for digital forensic investigation concepts still present challenges (Sikos 2021: e1394).

The development and advancement of networks and communication have helped IoT (Internet of Things) technology to connect and communicate billions of things via the Internet. IoT connects almost all physical and virtual objects in the world through the Internet. However, along with the advantages it provides, this technology introduces new issues, especially in the field of security, and highlights an IoT-based investigative framework as one of the highest priorities for every organization (Atlam et al. 2020: 551-577).

To examine digital evidence, forensic agencies and law enforcement use various digital forensic tools, and research by a group of authors focuses on identifying current state-of-the-art digital forensic concepts and existing research. Their research provides a comparative analysis based on the characteristics of various tools to help investigators choose tools during the forensic process (Javed et al. 2022: 11065-11089).

As cybercrime has become one of the most urgent topics that police organizations have been dealing with in recent years, one of the key challenges is how to best understand and effectively convey relevant skills and knowledge about cybercrime across the organization, i.e., enabling police officers to respond appropriately to such illicit behavior. Research conducted on this topic indicates that police officers consider some training methods to be significantly more effective than others, while also highlighting some of the organizational contexts that negatively impact the pro-

vision of effective cyber training to police officers. The analysis conducted through a survey showed that online learning is not considered as effective as other forms of learning delivery, although this method can be useful when it comes to upgrading skills (Cockcroft et al. 2021: 15-33).

The development of forensic tools specialized in identifying key elements of cyberattacks is necessary, and research results indicate that there are many tools that need to be updated to bridge the gap and find an appropriate and comprehensive tool that will address all the key elements of cybercrime: the criminal, the tool, and the victim (Dweikat et al. 2020).

Theoretical background

The research question "How does the age and education of users in Croatia affect their level of caution and sence of security when making online payments in digital banking?" is grounded in the sociotechnical systems theory paradigm. This theory emphasizes the interrelationship between social and technical elements within a system, particularly relevant to technology use and cybersecurity (Bostrom & Heinen, 1977: 341-357). Key aspects of Sociotechnical Systems Theory relevant to the research question are:

- Interaction of Social and Technical Elements: Sociotechnical systems theory posits that human behavior, including perceptions and interactions with technology, is influenced by social factors such as demographics, as well as technical characteristics (Trist & Bamforth, 1951: 3-38; Mumford, 2006: 317-342).
- Customization of Technological Solutions: Sociotechnical theory suggests that solutions should be tailored to users' social contexts. Findings from the research could guide the development of cybersecurity strategies tailored to different demographic groups (Bostrom & Heinen, 1977: 341-357).

However, it can be also analyzed through multiple paradigms:

- Sociotechnical Paradigm: This paradigm focuses on the interaction between social and technical systems, emphasizing how demographic factors influence user interactions with technology (Bostrom & Heinen, 1977: 341-357).
- Cognitive Paradigm: This approach examines how cognitive processes such as information processing and mental models affect cybersecurity behaviors across different demographic groups (Fogg, 2003; Norman, 2013).
- Diffusion of Innovations Theory: Rogers' theory explains how different demographic groups adopt and perceive new technologies and practices, including cybersecurity measures (Rogers, 2003).

- Social Constructivist Paradigm: This paradigm explores how social interactions and cultural norms shape users' understanding of cybersecurity, influenced by demographic factors (Vygotsky, 1978; Berger & Luckmann, 1966).

Consequently, the research problem of this study is not strictly tied to one paradigm. While a sociotechnical paradigm might be a strong fit given the focus on the interaction between users and technology, other paradigms like cognitive, diffusion of innovations, and social constructivism also offer valuable insights. Each paradigm provides a different perspective on how demographic factors might influence cybersecurity perceptions and behaviors, making it beneficial to consider multiple paradigms in our analysis.

Research methodology and hypothesis

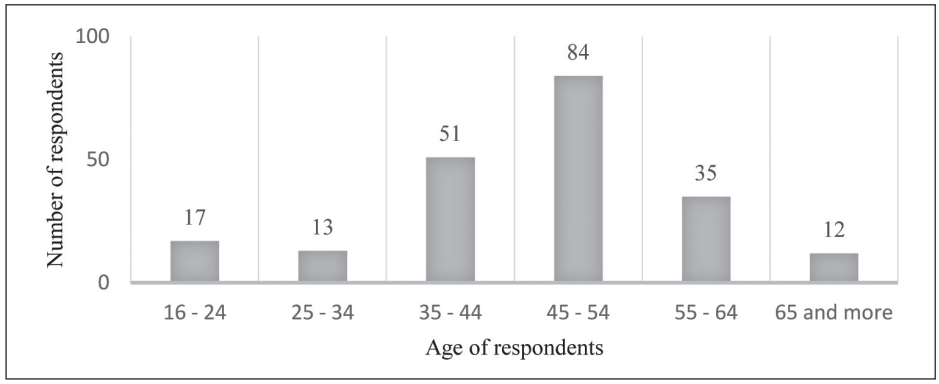
Methodology

The research for this paper was carried out with an online survey in Qualtrics conducted by postings on social networks Facebook, LinkedIn and Twitter, and by sending the survey by e-mail to target groups who are currently attending high school and university education or are already employed. The research included 212 respondents divided into six age groups. The sample (n=212) was realized with 100% response quality, and with a standard deviation of 0%. The survey questions were compiled by the author of the paper, a combination of different types of questions was used in order to get a comprehensive picture of respondents' perceptions and attitudes towards cyber security, and below is a brief overview of the types of questions used.

212 respondents of different age groups started filling out the online survey, and the largest number of respondents are from the age group between 45 and 54 years old, as can be seen from Graph 1. 64.62% of the respondents are female, and all the rest are male.

75,47% of users recognize the definition that best describes the term cyber security (Graph 2).

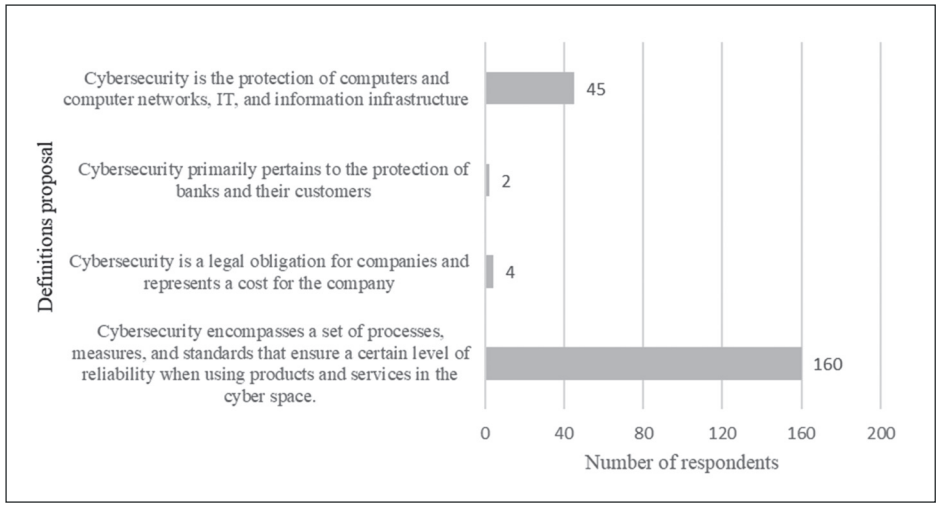
Pensioners were identified as the most vulnerable group in terms of exposure to cyber fraud (64.62%), while the least vulnerable are working respondents, 8.96% of whom are under 20 years old (9.43%). The rest refers to people with a lower level of education (Graph 3).



Authors of the paper

Graph 1. Which age group do you belong to?

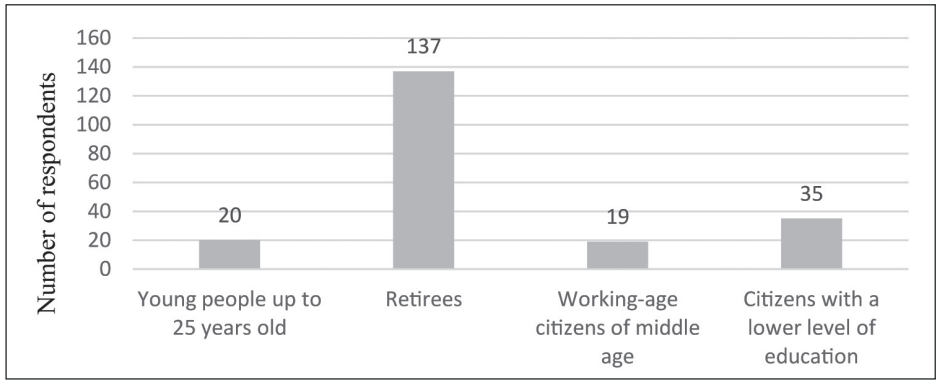
Grafikon 1. Kojoj dobnoj skupini pripadate?



Authors of the paper

Graph 2. Which definition, in your opinion, best describes the term cybersecurity?

Grafikon 2. Koja definicija prema vama najbolje opisuje pojam kibernetička sigurnost?



Authors of the paper

Graph 3. Which age groups do you consider the most vulnerable to cyber fraud?

Grafikon 3. Koje dobne skupine smatrate najranjivijima s obzirom na izloženost kibernetičkim prijevarama?

Out of a total of 212 respondents, 205 of them use the internet daily, and only 3.30% of respondents use the internet rarely, when necessary or 2-3 times a week. Not a single respondent stated that they never use the internet, which corresponds to the way the survey was conducted. 32.55% of respondents use internet banking services when necessary, 31.13% every day, as well as those who do it 2-3 times a week. 2.36% of respondents rarely use Internet banking, while only 1.89% of respondents never use Internet banking services.

To test the impact of users' age on the level of caution during online payments, a multiple regression analysis was used. This method allows for the estimation of the effect of the independent variable (age) on the dependent variable (caution in online payment), while controlling for other variables such as education and income.

- **Dependent variable (Y)**: How secure the respondents feel when paying online, measured using a Likert scale from 1 to 5 (1 = completely careless, 5 = extremely cautious).
- **Independent variable (X)**: User age, categorized into two groups: younger users (up to 34 years) and older users (45 years and above).
- **Control variables (Z)**: Education and eployment status, as potential factors that may affect the results.

The mathematical form of the regression model:

$$Y=\beta0+\beta1X+\beta2Z1+\beta3Z2+\epsilonY = \beta_0 + \beta_1X + \beta_2Z_1 + \beta_3Z_2 + \epsilonY=\beta0+\beta1X+\beta2Z1+\beta3Z2+\epsilon$$

where Y is the level of caution, X is the age group, Z1Z_1Z1 is education, and Z2Z_2Z2 is income. β1\beta_1β1 represents the coefficient that measures the impact of age on the level of caution, whereas Multiple Regression enables the assessment of the influence of several variables on the dependent variable.

The research was conducted with the Qualtrics online tool (www.qualtrics.com) in the period from May 13 to 27, 2024, and it took an average of 3 minutes and 30 seconds to complete the survey. Before publishing the survey a pilot study was conducted on 5 subjects of different age groups (n=10) for whom the questions were clear and understandable. The literature review was carried out in the same period. The methodological limitations of the work are based on the use of a quantum sample of non-probabilistic research, so the generalization of the results from the sample to the population with a known level of sample error is impossible.

Research hypotheses

The research question: How does the age and education of users in Croatia affect their level of caution and sence of security when making online payments in digital banking?*,* lead to the following hypotheses:

Hypothesis 1 (H1): Older users (aged 45 and above) exhibit a higher level of caution when making online payments compared to younger users (up to 44 years old).

Hyothesis 2 (H2): A higher level of education positively affects users' sense of security when paying online with bank cards.

Research issues and challenges

In the context of previous research and theories, several issues and challenges can be identified where the current study might have "hooked" or encountered problems with the research questions and hypotheses that were set. These challenges often stem from theoretical assumptions, methodological approaches, and interpretations of findings. Here are the key areas where the research may have faced difficulties:

Theoretical Alignment and Assumptions

- Demographic Factors and Cybersecurity: The study's assumption that demographic factors, particularly age, significantly influence cybersecurity percep-

tions may be questioned. The results suggest that age might not be as critical a factor as initially hypothesized. This raises questions about the adequacy of the theoretical framework in capturing user behavior complexity (Venkatesh et al., 2003: 425-478; Davis, 1989: 319-340).

Operationalization of Concepts

- Cybersecurity Perception Measurement: The study's measurement of cybersecurity perception might not capture its full multidimensional nature. Simplistic questions or those not aligned with users' real experiences could skew results (Kankanhalli et al., 2003; Davis, 1989).
- Age as a Binary Variable: Dividing age into binary categories might oversimplify the analysis. Age is a continuous variable, and such simplification can mask important variations within age groups (Stevens, 2017;).

Interpretation and Generalization of Results

- Overgeneralization of Findings: The mixed and sometimes contradictory results from various analyses (e.g., no significant findings in initial tests but significant results in further analysis) suggest that the research might have been prone to overgeneralization. When findings from different tests conflict, attempting to draw broad conclusions can undermine the study's validity (Cohen, 1994; Schmidt, 1996: 301-307). Overgeneralizing, especially in the absence of consistent evidence across various tests, may lead to misleading conclusions about the relationships between demographic factors and cybersecurity behaviors (Ioannidis, 2005: e124).
- Neglecting Contextual Factors: The study may have underestimated the impact of contextual factors, such as specific characteristics of the Croatian digital banking environment or broader socio-economic trends, on cybersecurity perceptions and behaviors. By focusing predominantly on demographic factors, the research might have missed significant contextual influences that could explain observed behaviors (Teddlie & Tashakkori, 2009; Yin, 2018). The failure to account for these factors could limit the applicability and relevance of the findings in different contexts.

Theoretical Contributions and Paradigmatic Fit

- Paradigmatic Limitations: The study may have been constrained by adhering too closely to a single theoretical paradigm, such as a behavioral or demographic fo-

cus, without exploring alternative paradigms. For instance, integrating insights from socio-technical systems theory or cultural studies could provide a more comprehensive understanding of how users perceive and engage with cybersecurity (Trist & Bamforth, 1951: 3-38). To consider multiple paradigms can offer richer insights into the complex interplay between demographic factors and cybersecurity practices.

The research faced several challenges related to theoretical assumptions, methodological choices, and operational definitions. To enhance the robustness of future studies, it is crucial to broaden the theoretical framework, employ more representative sampling methods, refine concept measurement, and avoid overgeneralization. Additionally, adopting a multi-paradigmatic approach could reveal deeper insights into the intricate relationship between demographic factors and cybersecurity perceptions in digital banking (Creswell & Creswell, 2017; Saunders et al., 2016).

Results

Research results and valorization of hypotheses

From the research carried out on 212 subjects, dependent and independent and control variables were singled out, on the basis of which a multiple regression analysis was made, and they are:

- **Dependent variable (Y)**: How secure the respondents feel when paying online, respectively level of caution in online payments, measured using a Likert scale from 1 to 5 (1 = completely careless, 5 = extremely cautious). This variable is dependent because it measures the user's feeling of security during online payments, and the goal is to investigate what influences this feeling.
- **Independent variable (X)**: User age, categorized into two groups: younger users (up to 44 years) and older users (45 years and above). This is an independent variable that measures the age of the user. It is a continuous or ordinal variable (depending on how the data is entered) and is used to analyze the impact of age on the feeling of security.
- **Control variables (Z)**: Education and employment status, as potential factors that may affect the results. Level of Education (Z1) as independent variable refers to the education level of the respondents. It is an ordinal variable as it measures the levels of education (1 = lower education, 7 = higher education). Additionaly, emplyoment status describes the socio-economic status of the respondents. It is also an ordinal variable, with values representing different levels of status (1 = lower status, 4 = higher status).

Table 1 shows the results of the multiple regression analysis, and the results obtained in the context of the set hypotheses can be interpreted as follows:

Table 1. Regresijska analiza

Table 1. Regression analysis

Regression Statistics	
Multiple R	0,276428497
R Square	0,076412714
Adjusted R Square	0,063027391
Standard Error	0,919163362
Observations	211

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	3	14,4691638	4,823054613	5,708694063	0,000898013
Residual	207	174,886286	0,844861287		
Total	210	189,35545			

		Coefficients	*tandard Errc*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95,0%*	*Upper 95,0%*
Intercept		3,647432166	0,2930983	12,44439874	6,58559E-27	3,069591676	4,225272656	3,069591676	4,225272656
	4	-0,09853908	0,06592551	-1,494703315	0,136514753	-0,228510592	0,031432432	-0,228510592	0,031432432
	7	0,097306319	0,0418591	2,324615551	0,021061883	0,014781502	0,179831135	0,014781502	0,179831135
	2	-0,168623114	0,12417904	-1,357903137	0,17597273	-0,413440907	0,076194679	-0,413440907	0,076194679

Authors of the paper

Hypothesis 1 (H1): Older users show a lower sense of security when paying online compared to younger users.

- This hypothesis is based on the negative coefficient for age (-0.099), although this result is not statistically significant (p = 0.137). However, for theoretical reasons we can make this hypothesis, because previous research often indicates that older users have less security or trust in technologies.
- Older users show a lower sense of security when paying online compared to younger users.
- Result: This hypothesis is rejected.
- Coefficient for age (β1): -0.099 (a negative sign suggests that older users feel less secure, which supports the hypothesis).
- p-value: 0.137 (which is more than 0.05), which means that this result is not statistically significant. Although there is a negative relationship between age and feeling safe, this relationship is not strong enough to be considered significant.

Hypothesis 2 (H2):A higher level of education positively affects users' sense of security when paying online with bank cards.

- This hypothesis stems from the fact that education showed a statistically significant and positive influence on the dependent variable ($p = 0.021$; coefficient = 0.097). Users with a higher level of education tend to feel more secure when making online payments.
- A higher level of education has a positive effect on users' sense of security when paying online with bank cards.
- Result: This hypothesis was confirmed.
- Coefficient for education ($\beta 2$): 0.097 (positive sign indicates that education increases the feeling of security).
- p-value: 0.021 (which is less than 0.05), which means that the influence of education is statistically significant. Thus, users with higher education really feel more secure when paying online.

Discussion

The results of the survey conducted on 212 respondents of different age groups show that Croatian citizens are well acquainted with the concept of cyber security, as 194 of them answered positively to the question Q6 - Are you familiar with the concept of cyber security. 205 respondents use the Internet daily, and slightly more than 30% of respondents use Internet banking services every day. Pensioners were identified as the most vulnerable group exposed to cyber fraud, while working respondents and those under 20 are the least vulnerable.

The research examined the influence of age on various aspects of internet use, frequency of internet use for banking services, recognition of the concept of cyber security and respondents' behavior related to online banking and the use of bank cards for online payments.

Furthermore, based on the formulated research question, the specific aim of this study was to examine how age, education, and user status influence their sense of security in the context of digital banking The results of the multiple regression analysis provide insight into the impact of various demographic variables on users' sense of security when making online payments with bank cards. The results showed that education has a significant and positive impact on the sense of security during online payments. Users with higher levels of education demonstrated greater confidence in the security of online transactions. This is confirmed by a statistically significant coefficient ($\beta = 0.097$) and a p-value of 0.021, indicating that more

educated users better understand the technology and risks associated with online payments, resulting in an increased sense of security. This finding is consistent with previous research that highlights a positive relationship between education and technological literacy, contributing to greater trust in digital financial services.

Although it was expected that age would have a significant impact on the sense of security during online payments, the results did not confirm this. The coefficient for age was negative ($\beta = -0.099$), suggesting that older users exhibit slightly lower levels of security compared to younger users, but this difference was not statistically significant ($p = 0.137$). This result suggests that age is not a key factor in explaining users' sense of security, at least in this sample. However, it is possible that other factors (e.g., previous experience with online payments or technical support) could better explain why older users may feel less secure, which could be the subject of further research.

As for employment status, the results showed that this variable is not a significant predictor of security in online payments ($p = 0.176$). Although the coefficient for status was negative ($\beta = -0.169$), indicating that users with lower socio-economic status exhibit lower levels of security, this effect was not statistically significant. This finding aligns with the hypothesis that socio-economic status by itself is not a strong enough factor to significantly influence the perception of security in online payments.

While the results showed statistically significant relationships for education, it is important to note that the R^2 value was only 0.076, indicating that only about 7.6% of the variation in the sense of security can be explained by age, education, and status. This suggests that many other factors not included in this model are also important in explaining the perception of security during online payments. Factors such as trust in technology, previous experiences with fraud, or risk perceptions likely play an important role and should be included in future research.

Conclusion

This study examined the impact of demographic factors on users' sense of security when making online payments with bank cards. Based on the conducted regression analysis, we can conclude the following: Education proved to be a significant predictor of the sense of security, with users who have higher levels of education showing a greater sense of security when making online payments. Age and status did not prove to be statistically significant factors in explaining the sense of security among users in this sample, although age had a negative impact, suggesting that older users may feel somewhat less secure, but without strong enough evidence.

Model limitations: The relatively low \(R^2\) value suggests that a significant portion of the variation in the perception of security remains unexplained by this model. Future research should include a broader range of variables, such as technological literacy, trust in online banking, and personal experiences with online fraud, to obtain a more comprehensive picture of the factors influencing security in digital banking. In conclusion, while education plays a key role in increasing security during online payments, further research should explore a wider context and the roles of other demographic, psychological, and technical factors to better understand users' perceptions of security in digital banking.

Overall the research indicates that while age affects certain cybersecurity-related behaviors, such as caution during online payments and recognition of cybersecurity importance, it does not significantly influence other behaviors like internet usage frequency or bank card use for online transactions. This suggests that cybersecurity strategies should be customized for different age groups, with an emphasis on enhancing awareness and promoting cautious behavior, particularly among younger users (Ajzen, 1991: 179-211; Rogers, 2003).

REFERENCES

Adams, R., Brown, S. & J. Taylor (2022) "The impact of demographic factors on digital behavior", *Journal of Cybersecurity*, 15 (3), 45–62. doi: 10.1007/978-3-030-29374-1_54.

Al-Alawi, A. I. & M. S. A. Al-Bassam (2020) "The significance of cybersecurity system in helping managing risk in banking and financial sector", *Journal of Xidian University*, 14 (7), 1523–1536. doi: 10.37896/jxu14.7/174.

Ajzen, I. (1991) "The Theory of Planned Behavior. Organizational Behavior and Human Decision", *Processes*, 50 (2), 179–211. doi: 10.1016/0749-5978(91)90020-T.

Alkhowaiter, W. A. (2020) "Digital payment and banking adoption research in Gulf countries: A systematic literature review", *International Journal of Information Management*, 53, 102102. doi: 10.1016/j.ijinfomgt.2020.102102.

Antoliš, K. (2024) "Education against Disinformation", *Interdisciplinary Description of Complex Systems*: *INDECS*, 22 (1), 71–83. doi: 10.7906/indecs.22.1.4.

Atlam, H. F., Alenezi, A., Alassafi, M. O., Alshdadi, A. A. & G. B. Wills (2020) "Security, cybercrime and digital forensics for IoT", *Principles of internet of things (IoT) ecosystem: Insight paradigm*, 551–577. doi: 10.1007/978-3-030-33596-0_22.

Back, S. & R. T. Guerette (2021) "Cyber place management and crime prevention: the effectiveness of cybersecurity awareness training against phishing

attacks", *Journal of Contemporary Criminal Justice*, 37 (3), 427–451. doi: 10.1177/10439862211001628.

Berger, P. L. & T. Luckmann (1966) *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. New York: Anchor Books. ISBN: 0-385-05898-5.

Bostrom, R. P. & J. S. Heinen (1977) "MIS problems and failures: A socio-technical perspective", *ACM Transactions on Information Systems*, 1 (4), 341–357.

Broby, D. (2021) "Financial technology and the future of banking", *Financial Innovation*, 7 (1), 47. doi: 10.1186/s40854-021-00264-y.

Camillo, M. (2017) "Cybersecurity: Risks and management of risks for global banks and financial institutions", *Journal of Risk Management in Financial Institutions*, 10 (2), 196–200.

Cartwright, A., Cartwright, E. & E. S. Edun (2023) "Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies", *Computers & Security*, 131, 103288. doi: 10.1016/j.cose.2023.103288.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S. et al. (2023). „Exploring the global geography of cybercrime and its driving forces". *Humanities and Social Sciences Communications*, 10(1), pp. 1–10. doi: 10.1057/s41599-023-01560-x.

Cohen, J. (1994) *The Earth is round (p < .05). Statistical Power Analysis for the Behavioral Sciences (2nd ed.)*. New Jersey: Lawrence Erlbaum Associates. ISBN: 978-0805802832.

Creado, Y. & V. Ramteke (2020) "Active cyber defence strategies and techniques for banks and financial institutions", *Journal of Financial Crime*, 27 (3), 771–780. doi: 10.1108/JFC-01-2020-0008.

Creswell, J. W. & J. D. Creswell (2017). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Los Angeles: Sage Publications. ISBN: 978-15063867056.

Culnan, M. J., & P. K. Armstrong (1999) "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation", *Organization Science*, 10 (1), 104–115. doi: 10.1287/orsc.10.1.104.

Cockcroft, T., Shan-A-Khuda, M., Schreuders, Z. C. & Trevorrow, P. (2021). „Police cybercrime training: perceptions, pedagogy, and policy". *Policing: A Journal of Policy and Practice*, 15(1), pp. 15–33. doi: 10.1093/police/pay078.

Davis, F. D. (1989) "Perceived usefulness, perceived ease of use, and user acceptance of information technology", *Management Information Systems Quarterly*, 13 (3), 319–340. doi: 10.2307/249008.

Datta, P., Panda, S. N., Tanwar, S. & Kaushal, R. K. (2020) A technical review report on cyber crimes in India, 269–275. In: *2020 International conference on emerging smart computing and informatics (ESCI)*. Pune, India: IEEE. doi: 10.1109/ESCI48226.2020.9167567.

Demirkan, S., Demirkan, I. & A. McKee (2020) "Blockchain technology in the future of business cyber security and accounting", *Journal of Management Analytics*, 7 (2), 189–208. doi: 10.1080/23270012.2020.1731721.

Diener, F. & M. Špaček (2021) "Digital transformation in banking: A managerial perspective on barriers to change", *Sustainability*, 13 (4), 2032. doi: 10.3390/su13042032.

Do, T. D., Pham, H. A. T., Thalassinos, E. I. & H. A. Le (2022) "The impact of digital transformation on performance: Evidence from Vietnamese commercial banks", *Journal of Risk and Financial Management*, 15 (1), 21. doi: 10.3390/jrfm15010021.

Dweikat, M., Eleyan, D. & A. Eleyan (2020) "Digital Forensic Tools Used in Analyzing Cybercrime", *Journal of University of Shanghai for Science and Technology*, 23 (3), 367–379. doi: 10.51201/Jusst12621.

Fogg, B. J. (2003) *Persuasive Technology: Using Computers to Change What We Think and Do*aSan Francisco: *Morgan Kaufmann*. ISBN: 1-55860-643-2.

Galinec, D., Možnik, D. & B. Guberina (2017) "Cybersecurity and cyber defence: national level strategic approach", *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, 58 (3) 273–286. doi: 10.1080/00051144.2017.1407022.

Ghelani, D. (2022) "Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review", *American Journal of Science, Engineering and Technology*, 3 (6), 12–19.

Gulyás, O. & G. Kiss (2023) "Impact of cyber-attacks on the financial institutions", *Procedia Computer Science*, 219, 84–90, available at: https://www.sciencedirect.com/science/article/pii/S1877050923002752, accessed 26 6. 2024.

Hasan, M. F. & N. S. Al-Ramadan (2021) "Cyber-attacks and cyber security readiness: Iraqi private banks case", *Social Science and Humanities Journal (SSHJ)*, 2312–2323. doi: 10.6084/m9.figshare.15190185.v2.

Hellvig, R., DUMITRESCU, C. & M. Dumitrescu (2020) "Management of Cybercrime in the Financial Field-Perspectives to Combat the Phenomenon", *Internal Auditing & Risk Manage*ment, 59 (3), 23–33, available at: https://ideas.repec.org/a/ath/journl/v59y2020i3p23-33.html, accessed 24. 6. 2024.

Holt, T. J., Bossler, A. M. & K. C. Seigfried-Spellar (2022) *Cybercrime and digital forensics: An introduction (3rd ed.)*. New York: Routledge. ISBN: 978-0367360078.

Ioannidis, J. P. A. (2005) "Why most published research findings are false", *PLoS Medicine*, 2 (8), e124. doi: 10.1371/journal.pmed.0020124.

Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K. & T. R. Gadekallu (2022) "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions", *IEEE Access*, 10, 11065–11089. doi: 10.1109/ACCESS.2022.3142508.

Jin, J., Li, N., Liu, S. & Nainar, S. K. (2023). „Cyber attacks, discretionary loan loss provisions, and banks' earnings management". *Finance Research Letters*, 54, p. 103705. doi: 10.1016/j.frl.2023.103705.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y. & K. K. Wei (2003) "An integrative study of information systems security effectiveness", *International Journal of Information*, 23 (2), 139–154. doi: 10.1016/S0268-4012(02)00105-6.

Kaur, S. J., Ali, L., Hassan, M. K. & M. Al-Emran (2021) "Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts", *Journal of Financial Services Marketing*, 26, 107–121. doi: 10.1057/s41264-020-00082-w.

Katterbauer, K., Syed, H. & Cleenewerck, L. (2022). „Financial cybercrime in the Islamic finance metaverse". *Journal of Metaverse*, 2(2), pp. 56–61. doi: 10.57019/jmv.1108783.

Khan, H. U., Malik, M. Z., Nazir, S. & F. Khan (2023) "Utilizing bio metric system for enhancing cyber security in banking sector: a systematic analysis", *IEEE Access*, 11 (80181–80198). doi: 10.1109/ACCESS.2023.3298824.

Kitsios, F., Giatsidis, I. & M. Kamariotou (2021) "Digital transformation and strategy in the banking sector: Evaluating the acceptance rate of e-services", *Journal of Open Innovation: Technology, Market, and Comp*lexity, 7 (3), 204. doi: doi.org/10.3390/joitmc7030204.

Kumar, M. (2023) "An overview of cyber security in digital banking Sector", *East Asian Journal of Multidisciplinary Research*, 2 (1), 43–52. doi: 10.55927/eajmr.v2i1.1671.

Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H. & T. Vasilyeva (2022) "Countering cybercrime risks in financial institutions: Forecasting information trends", *Journal of Risk and Financial Management*, 15 (12), 613. doi: 10.3390/jrfm15120613.

Manoj, K. S. (2021) "Cyber risk in banking services: the extent of cyber risks provisions and security measures", *International Journal of Management (IJM)*, 12 (1), 1332–1339. doi: 10.34218/IJM.12.1.2021.117.

Mhlanga, D. (2020) "Industry 4.0 in finance: the impact of artificial intelligence (ai) on digital financial inclusion", *International Journal of Financial Studies*, 8 (3), 45. doi: 10.3390/ijfs8030045.

Mittal, S. & P. V. Ilavarasan (2019) Demographic factors in cyber security: an empirical study, 667–676. In: *Digital Transformation for a Sustainable Society in the 21st Century: 18th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, I3E 2019, Trondheim, Norway, September 18–20, 2019, Proceedings 18*. Heidelberg: Springer International Publishing. doi: 10.1007/978-3-030-29374-1_54.

Mumford, E. (2006) "The story of socio-technical design: Reflections on its successes, failures, and potential", *Information Systems Journal*, 16 (4), 317–342. doi: 10.1111/j.1365-2575.2006.00221.x.

Norman, D. A. (2013) *The Design of Everyday Things: Revised and Expanded Edition*. New York: Basic Books. ISBN: 978-0465050659

Panja, B., Fattaleh, D., Mercado, M., Robinson, A. & P. Meharia (2013) Cybersecurity in banking and financial sector: Security analysis of a mobile banking application, 397–403. In: *2013 International Conference on Collaboration Technologies and Systems (CTS).* San Diego: IEEE. doi: 10.1109/CTS.2013.6567261.

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J. & C. Zopounidis (2022) "Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework", *Research in International Business and Finance*, 60, 101616. doi: 10.1016/j.ribaf.2022.101616.

Rogers, E. M. (2003) *Diffusion of Innovations (5th ed.)*. New York: Free Press. ISBN: 978-0743222099

Saunders, M., Lewis, P. & A. Thornhill (2016) *Research Methods for Business Students (7th ed.)*. Harlow: Pearson Education. ISBN: 978-1292016627.

Schmidt, F. L. (1996) "Statistical significance testing and cumulative knowledge in psychology: Implications for training of researchers", *Psychological methods*, 1 (2), 115. doi: 10.1037/1082-989X.1.2.115.

Sikos, L. F. (2021) "AI in digital forensics: Ontology engineering for cybercrime investigations", *Wiley Interdisciplinary Reviews: Forensic Science*, 3 (3), e1394. doi: 10.1002/wfs2.1394.

Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J. & T. Zema (2021) "Cybersecurity and sustainable development", *Procedia Computer Science*, 192, 20–28. doi: 10.1016/j.procs.2021.08.003.

Stanikzai, A. Q. & M. A. Shah (2021) Evaluation of cyber security threats in banking systems, 1–4. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)*. Orlando: IEEE. doi: 10.1109/SSCI50451.2021.9659862.

Stevens, J. P. (2017) *Intermediate Statistics: A Modern Approach (3rd ed.)*. New York: Routledge. ISBN: 978-0805854664.

Škiljić, A. (2020) "Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats", *International Cybersecurity Law Review*, 1, 51–61. doi: 10.1365/s43439-020-00014-30.

Teddlie, C. & A. Tashakkori (2009) *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Thousand Oaks: Sage Publications. ISBN: 978-0761930129.

Trist, E. L. & K. W. Bamforth (1951) "Some social and psychological consequences of the longwall method of coal getting", *Human Relations*, 4 (1), 3–38. doi: 10.1177/001872675100400010.

Tsindeliani, I. A., Proshunin, M. M., Sadovskaya, T. D., Popkova, Z. G., Davydova, M. A. & O. A. Babayan (2022) "Digital transformation of the banking system in the context of sustainable development", *Journal of Money Laundering Control*, 25 (1), 165–180. doi: 10.1108/JMLC-02-2021-0011.

Vinoth, S., Vemula, H. L., Haralayya, B., Mamgain, P., Hasan, M. F. & M. Naved (2022) "Application of cloud computing in banking and e-commerce and related security threats", *Materials Today: Proceedings*, 51, 2172–2175. doi: 10.1016/j.matpr.2021.11.121.

Venkatesh, V., Morris, M. G., Davis, G. B. & F. D. Davis (2003) "User acceptance of information technology: Toward a unified view", *Management Information Systems Quarterly*, 27 (3), 425–478. doi: 10.2307/30036540.

Vygotsky, L. S. (1978) *Mind in Society: The Development of Higher Psychological Processes*. Cambridge: Harvard University Press. ISBN: 978-0674576292.

Wewege, L., Lee, J. & Thomsett, M. C. (2020) "Disruptions and digital banking trends", *Journal of Applied Finance and Banking*, 10 (6), 15–56.

Yin, R. K. (2018) *Case Study Research and Applications: Design and Methods*. Thousand Oaks: *Sage Publications*. ISBN: 978-1506336169.

Medij. istraž. (god. 30, br. 2) 2024. (129-52)

Utjecaj starosne dobi i obrazovanja na kibernetičku sigurnost u digitalnom bankarstvu

Manuela Bukovec
Krunoslav Antoliš

SAŽETAK

Kibernetička sigurnost predstavlja temelj očuvanja povjerljivosti i integriteta u suvremenom digitalnom dobu. Presudna je za sigurnost pojedinaca, organizacija i društva u cjelini. Na tim premisama temelji se ovaj rad koji istražuje utjecaj demografskih čimbenika na percepciju i ponašanje korisnika vezano uz kibernetičku sigurnost u digitalnom bankarstvu. Rad se oslanja na teoriju sociotehničkih sustava koja ispituje odnose između društvenih i tehničkih elemenata unutar uporabe tehnologije. Istraživanje je provedeno online anketom distribuirane objavama na društvenim mrežama Facebook, LinkedIn i Twitter, te slanjem ankete e-poštom ciljanim skupinama, koje se trenutačno školuju u sustavu srednjoškolskog i visokoškolskog obrazovanje ili su već zaposlene. U istraživanju je sudjelovalo 212 ispitanika podijeljenih u šest dobnih skupina, uzorak (n=212) je ostvaren sa stopostotnom kvalitetom odgovora i standardnom devijacijom od 0 %. Cilj istraživanja bio je razumjeti kako demografske karakteristike, posebice dob, utječu na interakcije s tehnologijom digitalnog bankarstva i praksama kibernetičke sigurnosti. Metodom višestruke regresije testirane su dvije hipoteze pri čemu je prva hipoteza (Stariji korisnici (od 45 i više godina) pokazuju veću razinu opreza pri online plaćanjima u usporedbi s mlađim korisnicima (do 44 godine)) odbačena, dok je druga hipoteza (Viši stupanj obrazovanja pozitivno utječe na osjećaj sigurnosti korisnika pri online plaćanju bankovnim karticama) potvrđena. Rezultati ukazuju na to da je obrazovanje značajan prediktor osjećaja sigurnosti, pri čemu korisnici s višim stupnjem obrazovanja pokazuju veći osjećaj sigurnosti prilikom online plaćanja. Dob i status nisu se pokazali kao statistički značajni čimbenici u objašnjenju osjećaja sigurnosti kod korisnika u ovom uzorku iako je dob imala negativan utjecaj, sugerirajući osjećaj manje sigurnosti starijih korisnika.

Ključne riječi: kibernetički kriminal, kibernetička sigurnost, digitalno bankarstvo, kibernetička prijevara, internetska plaćanja