SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 238

THE IMPORTANCE OF CYBERSECURITY AND ITS ROLE IN THE SUCCESSFUL IMPLEMENTATION OF E-SERVICES

Alicja FANDREJEWSKA-NOWAKOWSKA[1*], Robert NOWACKI[2], Kamil NOWACKI[3]

[1] Warsaw University of Life Sciences; alicja_fandrejewska@sggw.edu.pl, ORCID: 0000-0002-9189-1675
[2] VIZJA University in Warsaw; r.nowacki@vizja.pl, ORCID: 0000-0001-7380-0672
[3] Warsaw Management University; itwolfmaster@gmail.com, ORCID: 0009-0004-6276-2665
* Correspondence author

Purpose: This study aims to assess the awareness, knowledge and digital skills of young people, students from Warsaw universities, in the field of cybersecurity related to e-services. The survey investigates the respondents' awareness and knowledge related to various cyber threats, their perception, frequency and scale, and self-assessment of cybersecurity competence and practices.
Design/methodology/approach: The study involving 278 young e-consumers, students of universities in Warsaw, was conducted using a survey questionnaire (CAWI technique). The selection of the sample was purposive and convenient. Respondents were asked about their perception of cybersecurity threats, self-assessed ability to defend against attacks and their use of various cybersecurity measures. The research examined key variables such as gender, age (two groups: 19-22 and 23-26 years), employment status and place of residence (large vs. small city). Statistical analyses were performed using IBM SPSS Statistics 29.0
Findings: The results indicate high levels of cybersecurity awareness among young e-consumers. Many respondents recognize cyber threats and their potential consequences. However, they also lack confidence in their abilities and the effectiveness of cybersecurity measures and tools. The study highlights the gap between the awareness regarding cyber threats and practical skills or the ability to mitigate them effectively.
Research limitations/implications: The sample included a group of young e-consumers, students from major universities in Warsaw. Thus, the findings cannot be generalized to the broader population. However, due to their specific characteristics (level of education and digital skills, age and place of residence), the respondents may be regarded as a suitable group for pilot studies in cybersecurity awareness and skills development.
Practical implications: The findings indicate a need for adequately targeted educational initiatives to enhance cybersecurity competence and skills among young e-consumers.
Originality/value: This study examines the cybersecurity awareness of young people in the context of e-services, which is a topical yet underexplored issue. The study results can be valuable for educators, policymakers and cybersecurity professionals aiming to enhance cybersecurity awareness among young e-consumers.
Keywords: cybersecurity awareness and knowledge, digital skills, e-services, e-consumers, consumer safety.
Category of the paper: research paper.

Introduction

The rapid development of new technologies and the servitization of the economy have transformed many aspects of consumer functioning. The pandemic has also contributed to the development of new digital competencies among people of all ages. On the one hand, the immediate threat and fear for one's health and life, and on the other hand, the new opportunities and choices associated with the internationalization and globalization of services, have led consumers to increasingly turn to e-services instead of traditional services. As Wolny (2020, p. 90) states, "the emergence of electronic services (e-services), which refer to a form of service provision using the Internet, including, in particular, the presentation of the service, the ordering of the service, the payment for the service and the use of the service through this network, with the proviso that for selected services, their consumption takes place in the real (non-virtual) world". Due to the ubiquity of Internet access and the availability of technology in the form of platforms, systems and applications, e-services are becoming very popular among consumers. As Jaciow et al. (2015) emphasize, "the Internet is not only a primary source of information (informational function) but also an excellent place to conduct business (transactional function), including - selling products. From the consumer's point of view, the Internet is not just a source of information or an opportunity to spend leisure time. For modern consumers, the Internet is an opportunity to establish and maintain contact with others, engage in work and entertainment, but most importantly a place to make purchases and use e-services (regardless of where you live)" (Jaciow et al., 2015, p. 5).

As Kotlorz (2013, p. 7) points out, technological development determines the availability of e-services, but also increases the demand for them. More and more people are using a variety of communication channels, tools and instruments to access or purchase various types of services, such as: e-administration, e-banking, e-education, e-commerce, e-culture, e-tourism, e-insurance and e-health (Wolny, 2013, p. 23). As Jaciow et al. stress (2015, p. 5), the development of the e-services market "is determined by economic, demographic, social, cultural and technological factors. Technological changes are increasingly important for economic development, which translates into innovation of market players, both on the supply side (producers, intermediaries) and demand side (individual and institutional consumers)" (Jaciow et al., 2015, p. 5). As Wolny stresses (2013, p. 8), we may observe increased servitization, which is "associated with the increasing role of services in socio-economic relations, including an advanced stage of development of the service sector". Kotlorz (2013, p. 9) states that this development is affected by outsourcing and offshoring of services, technological progress, demographics, e.g. the ageing process and the changing structure of households, changes in labor productivity and the convergence of the service and manufacturing sectors. Jaciow et al. (2015, p. 5) stress that we are witnesses to "the virtualization of socio-economic life", and Papińska-Kacperek (2013, p. 132) emphasizes

the role of this sector stating that "all citizens are potential recipients of digital services". Given the scale and scope of the phenomenon, consumer safety and cybersecurity in e-services are important and topical issues that policymakers, practitioners and researchers need to consider and explore.

Safety of consumers is a very wide concept referring to consumer protection in terms of product safety and executing and protecting consumer rights, which is particularly important when dealing with power imbalance or information asymmetry (Kozłowska, 2019, pp. 107-109). According to Kozłowska (2019, pp. 107-109), the term also encompasses counteracting and punishing illegal, unethical and unfair market practices in terms of sales, advertising and marketing communications. Assessing the level of e-consumers' knowledge, awareness and competence is essential in order to provide them with resources and tools to execute their rights in the market (Dąbrowska et al., 2015; Bylok, 2019). Focusing on e-consumers' safety is crucial because the e-services market is becoming more difficult and more complex to navigate due to the development of new information and communication technologies (ICT), such as big data analytics, artificial intelligence (AI), including generative AI, virtual reality (VR) and augmented reality (AR) or Internet of Things (IoT). In addition, recommendation systems operating on the basis of artificial intelligence algorithms that analyze vast amounts of data about Internet users and gain valuable knowledge about e-consumers (Mróz, 2020, p. 66) can offer new opportunities, such as personalized recommendations, advertising and communications (Nowacki, Fandrejewska, 2024), convenience, time savings and streamlining of the decision-making process. However, they can also exploit the information (Nowacki, Fandrejewska, 2025) and vulnerability of e-consumers (Mróz, 2020, p. 69) or intensify the threats which are already there due to human nature and psychological constructs in humans like behavioral traps (Mruk, 2020, p. 28).

Unfortunately, the great popularity and widespread adoption of e-services expose users to cybersecurity threats. Cybercriminals exploit vulnerabilities in online platforms to gain unauthorized access to sensitive information. Also, cyberattacks can take many forms and they are designed to exploit different vulnerabilities in systems or networks functioning as part of digital economy (Boratyńska et al., 2021, p. 21). It is worth noting that user behavior can also be the reason why cybercriminals can infiltrate the network or the system. Realizing that threats may take many forms and disguises, e.g. malware (viruses, worms, trojans), ransomware, spyware, adware or phishing, the role of cybersecurity cannot be underestimated. Directives and regulations impose new compulsory procedures, tasks and responsibilities on corporations, intermediaries and service providers. However, as indicated earlier, responsibility for safeguarding digital interactions related to e-services lies not only with service providers but also with consumers, who must be aware, cautious and vigilant about protecting their data and resources.

As a recent report by the Warsaw Banking Institute (Postawy Polaków…, 2024) indicates, cybersecurity is increasingly important for e-consumers because they depend on digital services and develop a greater awareness of threats such as phishing (for personal data and money), identity theft, disinformation, and cyberbullying. According to recent statistics, the most feared online scams among Poles are phishing (60%), financial fraud (52%), identity theft (51%), disinformation and fake news (42%), and cyberbullying, including hate speech and violations of personal dignity (30%). Also, the recent EY Future Consumer Index data points to increasing consumers' concern related to data security; 61% of digital service users fear their information may lead to identity theft, up six percentage points in just one year. Concerns about the use of cookies and the potential misuse of personal information are now widespread among internet users, with 65% planning to pay more attention to company data policies, though 28% remain willing to share their data if in return they can receive more personalized offers (Olak, 2024).

The research problem presented in this paper is also discussed in other publications. Research by Alkis and Kose (2022) shows that privacy concerns and consumer characteristics shape how people approach online shopping and social media advertising across 29 European countries. The authors stress that higher privacy risk knowledge and greater online information sharing are linked to increased e-commerce activity, while strong concern about online activity recordings lowers participation; consumers who take more protective actions are more likely to shop online and respond to social media ads, making privacy protection tools valuable for companies in the digital market. A study conducted by Fortes and Rita (2016) in Portugal involving 900 respondents indicates that greater privacy concerns decrease trust and increase perceived risk, which in turn reduce consumers' willingness to make online purchases. The study confirms these effects using a research model based on trust and risk theories, planned behavior, and technology acceptance frameworks.

As Wahab et al. (2023) note, cybersecurity in e-commerce is important for building consumer trust and confidence because security policies and protection measures may influence users' willingness to shop online. However, as the authors emphasize, simply perceiving risks or having fears about cybercrime does not automatically discourage consumers from making purchases online. Another research by Sadab (2023) reveals that, for online shoppers in Bangladesh, cybersecurity knowledge, website quality, secure payment systems, and concern for data privacy significantly influence their attitudes toward e-commerce, while demographics like age and gender do not. The study highlights that consumers' awareness of cybersecurity risks increased during the Covid-19 pandemic and remains high, directly improving their trust and willingness to shop online. A study carried out by Singh et al. (2024), with the participation of 780 respondents, examines how consumers perceive different security mechanisms implemented on e-commerce platforms and analyzes how they influence the level of consumer trust. The latter is vital to consider because this dependence can later translate into their willingness to use such platforms. Similarly to our study, it also assesses the potential effects of gender and age. The survey by Singh also considered the frequency of e-commerce and

structural equation modeling (SEM). The findings indicate that information integrity and confidentiality have a strongly positive impact on consumer trust, and this trust mediates the relationship between these factors and consumers' intention to use e-commerce platforms. As the authors stress (Singh et al., 2024), contrary to expectations, there were no significant correlations between gender or age and how respondents perceived trust or security; however, it was discovered that "moderating effect of frequency of use on the relationship between perceived information confidentiality and preventing unauthorized secondary data usage on trusting beliefs was found to be significant". The research also points to critical safeguards that e-commerce platforms should develop to build user trust. Another study (Wisetpanich et al., 2025) based on a survey conducted among Gen Z representatives in Thailand, found that digital literacy including digital safety, content creation, and information management accounts for 77.5% of the variance in Generation Z's perceptions of data privacy security on Thai e-commerce platforms. Digital safety emerged as the most influential factor, and the findings highlight the importance of transparent data protection policies and tailored digital literacy initiatives aimed at strengthening user confidence and trust in online purchasing. Research conducted by Nguyen et al. (2024) reveals that digital literacy has a significant impact on both online security behaviors and the continued use of e-payments, with security behaviors serving as a mediator in the relationship between digital skills and users' willingness to continue using e-payment solutions.

New technologies emerge at an unprecedented pace, bringing numerous opportunities for innovation and progress. The fast development, increasing complexity and popularity of new technologies may result in the misuse of technology, and laws and legal regulations often lag behind, creating a gap that can lead to risks, vulnerabilities and potential threats. Ethical dilemmas and security concerns are serious issues raised by many experts, policymakers, business practitioners, researchers and users themselves. It is important to point out that even though cybersecurity is such an important and topical issue, very often the research on e-services cybersecurity is fragmented and focuses on narrow and highly specialized areas, like e-banking (Alrababah et al., 2024; Cele et al., 2024), retailers' loyalty programs (Chmielarz, Szumski, 2018), healthcare systems (Jalali et al., 2018; Ewoh, Vartiainen, 2024; Dąbrowska et al., 2025), public health (Mackey, Nayyar, 2016), smart cities (Adel, 2023) and administration and e-government (Hossain, 2024; Zhang, Kaur, 2024). The perspective of cybersecurity is more often examined from the standpoint of legal regulations or technological solutions. There are few studies that examine the competencies, knowledge, and skills of users themselves, even though these are crucial, as they can often improve the security and safety of consumers in the e-services market.

Rusayyis et al. (2022) state that "with the increasing importance of e-services in cyberspace, cybersecurity is essential for safety and trustworthiness. As Wolny (2020 after: Wasilewski, 2013, p. 233) indicates in general terms *cyberspace security* can be defined as "(...) a set of organizational, legal, technical, physical and educational measures aimed at ensuring the

uninterrupted functioning of cyberspace". In the context of e-services cybersecurity is a multidimensional concept which includes the security of devices, networks, applications, identity and access management (IAM), cryptography and social engineering defence. Stallings and Brown (2019, p. 27) stress the need for "protecting information systems by ensuring that data, software, and hardware stay safe, reliable, and accessible", and Cichosz (2017, p. 64) stresses that in the context of cybersecurity, apart from hardware and software, we should also consider the role of users interacting with cyberspace.

Analyzing the approach and behavior of individual users is very important from the point of view of ensuring the security of both technological solutions and systems which rely on them. Protection Motivation Theory (PMT) (Rogers, 1975), for instance, a theory which is commonly applied in research on cybersecurity behavior (Crossler et al., 2013; Sinopen et al., 2024), analyzes the relationship between protective behavior and threat assessment (its severity and vulnerability) and the assessment of one's own ability to cope with the threat (effectiveness of proposed actions, sense of self-efficacy, and costs of responding) (Kiran et al., 225). Users' decisions to take protective measures are determined by the extent to which they perceive the threat as serious and probable to occur, and their belief in the effectiveness of countermeasures and their own competence to apply them. It is worth noting that while this study does not directly apply Protection Motivation Theory (PMT), it is diagnostic in nature and its research questions address areas examined by PMT, such as threat awareness and perception, self-assessment of digital competence, sense of self-efficacy, and the need for digital skills education and improvement for oneself and others.

As indicated above, this issue can be analyzed from multiple perspectives. The studies can concentrate on cybersecurity-related behavior to improve understanding of the existing challenges and identify directions for further research (Almansoori et al., 2023), they may consider user behavior from the point of view of psychology, focus on individual differences that can influence cybersecurity practices, and recommend methods to improve user compliance with security policies (Moustafa et al., 2021). It is important to bear in mind that there exist factors which increase the risks associated with cybersecurity vulnerabilities that also need to be studied, e.g. new technologies like AI or IoT (Blessing et al., 2022), social engineering exploiting challenging circumstances like COVID-19 (Alzahrani, 2020) or multiple mobile entry points to systems, applications and devices (Ballagas et al., 2006 after: Cichosz, p. 69; Snopkiewicz, 2020, pp. 35-36)

Even though cybersecurity is a very important topic (Mocanu, 2013; Ćwiek, 2024; Oh, 2021; Lamond et al., 2022), the research is narrow in scope and fragmented, with few studies comprehensively analyzing the awareness, knowledge, and skills of young people in the context of cybersecurity. This research problem deserves attention because, contrary to expectations, despite young people spending a significant amount of time online and relying on their devices for many aspects of life, as research shows (Wilk, 2013, p. 25; Gwoździewicz,

2017 after: Gwoździewicz et al., 2025, p. 116), they do not always have sufficient practical cybersecurity skills or know how to protect themselves in cyberspace.

In their study, the authors attempted to assess the impact of various socio-demographic factors on the level of cybersecurity awareness and digital literacy among young people, users of e-services. The current study takes into account several factors that can potentially influence the level of cybersecurity awareness and digital skills: gender, age, education and place of residence. It is important to note that the selection of the research sample for the study was purposeful and convenient. Young people are a very important group of respondents due to their openness to new technologies, frequent use of various technological solutions, and level of advancement in terms of purchasing and using e-services. Analysis and assessment of the level of knowledge, digital skills, risk awareness and competence of e-consumers addresses a significant gap in cybersecurity research and may contribute to and support efforts to enhance cybersecurity and improve the safety of e-consumers in the market.

Methods

The issue of perception of cybersecurity was the subject of a CAWI survey conducted in October 2023 among young Poles. The study involved 278 people, diverse in terms of gender (56.8% women and 43.2% men), age (50.0% in two age groups: 19-22 and 23-26), professional activity (33.5% were full-time workers, 34.2% were working part-time and 32.4% were not working at all) and place of residence (divided into two categories: agglomerations with more than 2000 inhabitants or smaller towns - 65.1% and 34.9%, respectively). The sample selection was quota-based. The study was based on an original questionnaire consisting of five questions. Two questions, concerning knowledge about cyberattacks and the use of password managers, were closed-ended and based on simple nominal alternative scales. The next two questions concerned the security measures used by respondents and sources of information on cybersecurity – these questions were semi-open-ended and based on a conjunctive scale. The last question contained eight statements related to cybersecurity issues, which were evaluated on a five-point Likert scale. A seven-point scale was selected because of its proven advantages. Research shows that a smaller scale (e.g., 2- or 3-point) is not sufficiently detailed (Cox, 1980), while overly complex scales (e.g., 9- or 11-point) can weaken respondents' ability to differentiate values (Tarka, 2015). The validity and reliability of five- or seven-point scales have been confirmed by numerous studies (Alwin, 1997; Churchill, Peter, 1984; Matell, Jacoby, 1971; Schutz, Rucker, 1975). The questionnaire was developed on the basis of an analysis of literature sources and previous qualitative research, and was then pilot tested among a group of target respondents.

In the context of the described problem, the analysis focused mainly on the phenomena of knowledge about cyberattacks, the possibilities of protecting oneself against them and knowledge about cybersecurity. The results of the analyses were presented taking into account the variation due to four independent variables (gender, age, professional activity and place of residence). The relationships between the independent (explanatory) and dependent (explained) variables were determined using the non-parametric χ^2 test. All calculations were performed using IBM SPSS Statistics 29.0.

Results

The results obtained show that young consumers have a relatively high level of knowledge about cyberattacks occurring in their environment (Table 1). Every third person has come across information about such threats in the last 12 months. More than half have heard of at least one such attack. Only 12.2% indicated that they did not hear about any cyberattacks taking place in the last 12 months. In terms of specific correlation cross-sections, it should be noted that men, older age groups, full-time employees and residents of large urban areas are slightly more likely to declare greater knowledge of cyberattacks. The correlations between this question and the independent variables only occurred in the case of professional activity (employment status) and place of residence, but their strength is not high - the V-Cramér's coefficient does not exceed 0.2.

Table 1.
Knowledge about cyberattacks carried out in the last 12 months in general and according to the characteristics of the respondents

Specification	No, I haven't heard of it at all	Yes, I have heard of it a few times at most	Yes, I have heard of it many times	Test χ^2			Decision at p = 0.05
	Percentage share			Value (χ^2)	df	Critical level of significance (p)	
Gender				2.691	2	0.260	No dependency
Female	14.6	55.1	30.4				
Male	9.2	53.3	37.5				
Age				2.760	2	0.252	No dependency
19-22 years	15.1	54.7	30.2				
23-26 years	9.4	54.0	36.7				
Employment status				13.059	4	0.011	Weak dependency (Cramér's V coefficient = 0.153)
Not working	13.3	58.9	27.8				
Working part-time	11.6	63.2	25.3				
Working full-time	11.8	40.9	47.3				

Cont. table 1.

Place of residence				8.083	2	0.018	Weak dependency (Cramér's V coefficient = 0.171)
Town with up to 200,000 inhabitants	19.6	52.6	27.8				
City with up to 200,000 inhabitants	8.3	55.2	36.5				
Total	12.2	54.3	33.5	-	-	-	-

Source: own research, N = 278.

The respondents pointed out the need to increase the availability of cybersecurity education for consumers - almost 90% of respondents agree with this statement, with as many as half strongly agreeing with it. This is mainly due to the fact that more and more cyberattacks are being noticed and the belief that they threaten consumers' functioning. In the case of these two statements, the percentages of people agreeing are close to 80% and almost 90%. This is also confirmed by the fact that despite declaring knowledge of security measures and their use (compliance rates of 57.2% and 63.3%, respectively), the percentage of respondents indicating that their knowledge in this area is sufficient and the level of security is adequate is lower and amounted to approximately 34-36%. Every fourth respondent agrees with the statement that it is impossible to effectively protect against cyberattacks (Table 2).

Table 2.
Overall level of agreement with statements on cybersecurity

Specification	Strongly disagree	Rather disagree	Neither agree nor disagree / difficult to say	Rather agree	Strongly agree
	% share of indications				
Cybersecurity education should be more accessible to average consumers.	1.1	4.0	6.8	33.5	54.7
My cybersecurity skills are sufficient.	3.2	26.3	34.5	28.1	7.9
I am well protected against cyberattacks.	6.5	25.5	33.8	27.0	7.2
Cyberattacks are a growing threat to consumers.	0.7	2.5	10.1	37.1	49.6
The number of cyberattacks is constantly increasing.	0.7	3.2	16.2	42.4	37.4
There is no way to effectively protect against cyberattacks.	7.2	32.0	37.1	18.0	5.8
I know the security measures to protect my personal data and devices from cyberattacks.	5.0	14.4	23.4	46.0	11.2
I apply security measures to protect my personal data and devices from cyberattacks.	4.3	8.3	24.1	48.6	14.7

Source: own research, N = 278.

The analysis of statements on the assessment of cybersecurity knowledge level in relation to independent variables shows relatively little variation. Of the 32 variants (eight statements times four independent variables), the level of significance of the χ^2 test value did not exceed the critical value of p=0.05 in only eleven cases, indicating the existence of a statistical

relationship between the variables. It is characteristic that this concerns the independent variable "gender" in six cases - in all these cases, the value of the V-Cramér's coefficient ranges from 0.2 to 0.3, which means that there is a clear but low correlation. The highest value of the strength of the relationship was achieved in the case of the relationship between the statement "I am well protected against cyberattacks" and gender (0.261) - men declare this view much more often than women.

In the remaining five cases, a weak relationship was recorded four times (values between 0.171 and 0.195), and once a low relationship (value 0.227 - the relationship between the statement "The number of cyber-attacks is constantly increasing" and the variable "professional activity"). It is interesting to note that the weak relationship was three times higher for the statement "Cyberattacks are an increasing threat to consumers" and the only variable that showed no relationship was "gender" (Table 3).

Table 3.
Relationship between the degree of respondents' agreement with statements about cybersecurity and independent variables

Specification	Independent variable	χ^2 Test			Decision at p = 0.05
		Value (χ^2)	df	Critical significance level (p)	
Cybersecurity education should be more accessible to average consumers.	Gender	12.624	4	0.013	Weak dependency (V-Cramér's coefficient = 0.213)
	Age	5.058	4	0.281	No dependency
	Employment status	7.487	8	0.485	No dependency
	Place of residence	4.857	4	0.302	No dependency
My cybersecurity skills are sufficient.	Gender	18.453	4	0.010	Low dependency (V-Cramér's coefficient = 0.258)
	Age	0.945	4	0.918	No dependency
	Employment status	8.623	8	0.375	No dependency
	Place of residence	8.632	4	0.071	No dependency
I am well protected against cyberattacks.	Gender	18.868	4	<0.001	Low dependency (V-Cramér's coefficient = 0.261)
	Age	2.775	4	0.596	No dependency
	Employment status	16.332	8	0.038	Weak dependency (V-Cramér's coefficient = 0.171)
	Place of residence	6.086	4	0.193	No dependency
Cyberattacks are a growing threat to consumers.	Gender	6.006	4	0.199	No dependency
	Age	9.599	4	0.048	No dependency (V-Cramér's coefficient = 0.188)

	Employment status	17.561	8	0.025	Weak dependency (Cramér's V coefficient = 0.178)
	Place of residence	10.554	4	0.032	Weak dependency (V-Cramér's coefficient = 0.195)
The number of cyberattacks is constantly increasing.	Gender	9.360	4	0.053	No dependency
	Age	4.493	4	0.343	No dependency
	Employment status	28.772	8	<0.001	Low dependency (V-Cramér's coefficient = 0.227)
	Place of residence	1.452	4	0.835	No dependency
There is no way to effectively protect against cyberattacks.	Gender	12.949	4	0.012	Low dependency (V-Cramér's Coefficient = 0.216)
	Age	5.035	4	0.284	No dependency
	Employment status	7.598	8	0.474	No dependency
	Place of residence	6.502	4	0.165	No dependency
I know the security measures to protect my personal data and devices from cyberattacks.	Gender	17.577	4	0.001	Low dependency (V-Cramér's coefficient = 0.251)
	Age	2.826	4	0.587	No dependency
	Employment status	11.186	8	0.191	No dependency
	Place of residence	4.550	4	0.337	No dependency
I apply security measures to protect my personal data and devices from cyberattacks.	Gender	13.918	4	0.008	Low dependency (V-Cramér's coefficient = 0.224)
	Age	6.286	4	0.179	No dependency
	Employment status	3.100	8	0.928	No dependency
	Place of residence	1.493	4	0.828	No dependency

Source: own research, N = 278.

In response to the growing threat of cyberattacks, various measures are being taken to protect personal data and devices from hacking. Although not all respondents are fully aware of the existing protection options, all respondents have declared that they take measures related to cybersecurity. An overwhelming majority (90.3%) do not open suspicious links or attachments received by e-mail. When using multiple applications, it is common for examined e-consumers to use two-factor authentication, e.g. via codes received via SMS (80.8% of indications). Antivirus programs (71.9%), regular operating system and software updates, and complex passwords (69.1% of responses each) are also popular. Just over a third of respondents regularly change their passwords and one in five uses virtual private networks (VPNs). However, only 28.1% of respondents use password managers to manage their passwords.

The aforementioned issue of cybersecurity education is related to preferences regarding sources of information on this topic. The conducted research shows that the Internet and social media are of key importance in this area – over 95% of respondents obtain information from these sources. Almost half of the respondents obtained valuable information at work or at university, and a similar share valued the opinions of relatives or friends in this regard. However, as reported by study participants, the importance of other mass media, apart from the Internet or printed publications on cybersecurity, is low.

Discussion

The study results suggest that the surveyed group of young individuals demonstrates a relatively high level of knowledge and awareness regarding cyber threats and they also understand the importance of cybersecurity. The findings of this research indicate a growing concern among young consumers, students of Warsaw universities, regarding cybersecurity threats in the area of e-services. A significant number of respondents acknowledge an increasing frequency of cyberattacks and recognize their impact on consumer security in the area of purchasing and using e-services. On the one hand, this suggests a heightened awareness of the risks associated with online activities; on the other, it points to a sense of vulnerability in the face of these threats.

A significant proportion of respondents (one in three) reported encountering information about several cyberattacks within the past 12 months, and more than half had heard of at least one such incident. Only 12.2% of participants stated that they had not heard about cyberattacks at all, which further confirms the widespread awareness of digital threats.

Moreover, a statistically significant relationship was found between cybersecurity knowledge and specific demographic factors, including gender and age (men and slightly older respondents declared higher levels of knowledge regarding cyberattacks). A similar situation could be observed in the case of survey participants who declared full-time employment and residence in larger cities. Perhaps individuals who are already active in the job market are more aware of the cybersecurity risks and living in larger cities may be correlated with more exposure to information about cyberattacks or cybersecurity threats. However, the authors would like to note that while these relationships are statistically significant, their strength is not high. This indicates that while these factors influence cybersecurity awareness to some extent, other variables may also play a role regarding the level of cybersecurity knowledge and awareness or shaping attitudes toward cybersecurity.

An overwhelming majority of participants (nearly 90% agree, and around 50% strongly agree with the statements) emphasize the need for accessible cybersecurity education, which stresses the need recognized by respondents to expand their knowledge and improve their

digital safety skills. While a large share of respondents report knowing and adopting preventive measures (57% and 63% respectively), such as using two-factor authentication and updating antivirus software, their confidence in their cybersecurity knowledge or practical skills remains relatively low (around 35%). This demonstrates a gap between cybersecurity awareness and respondents' perceived competence in this area.

It is important to note that around 25% share of respondents believe that it is impossible to fully defend against cyberattacks, which may be a reason for concern because the sense of helplessness might be a discouraging factor for respondents to take initiatives like pursuing education opportunities, proactively developing practical cybersecurity skills or investing time, money and effort in building cybersecurity and safe use of devices, systems or platforms. The findings of the study point to the need to develop technical knowledge and devise strategies to enhance e-consumers' confidence in the effectiveness of cybersecurity practices. Addressing these issues using targeted educational initiatives could bridge the gap between e-consumers' awareness and their actions and behavior, which in turn will lead to the development of better cybersecurity habits among young users.

Summary

The study analyzes cybersecurity awareness, knowledge and practices among young e-consumers, students from Warsaw universities. The research findings indicate that nearly 90% of the respondents had encountered information about cyberattacks in the past year and many study participants reported using preventive measures and tools. However, the confidence of respondents regarding their cybersecurity knowledge remained cautious, with one in four believing cyberattacks cannot be fully prevented. The study results suggest a strong need for accessible cybersecurity education in order to bridge the gap between awareness and effective security practices and measures.

It is important to indicate that this study has certain limitations that should be considered. The use of a purposive and convenient sample does not allow for the findings to be generalized beyond the surveyed group. While some correlations were found, i.e. higher cybersecurity awareness among men, older individuals, full-time employees and urban residents, they were relatively weak. Also, self-reported data may not always reflect actual behaviors since increased media coverage and popularity of the topics related to cyberattacks or cyber threats may lead to higher awareness among young e-consumers; however, as the findings of the study suggest, it may not necessarily translate into practical skills or proactive security measures undertaken by this group.

As cyberattacks and cyber threats become more frequent, complex and widespread, e-consumers must expand their knowledge and develop effective cybersecurity practices. Well-informed and proficient users can recognize and prevent, or at least mitigate, potential cyber risks or threats. The awareness and preventive measures play a key role in increasing cybersecurity resilience, both on a personal and organizational level. It is also important to indicate that individual actions can contribute to greater security of networks, systems, and platforms and reduce threats and risks associated with cyberattacks.

Future research should expand its scope to examine cybersecurity awareness, knowledge, skills and behaviors across different populations. Further studies on cybersecurity should also include respondents from smaller towns and rural areas. The studies involving different samples could explore how access to digital resources and technological solutions or cybersecurity education opportunities influence both users' awareness and practices they learn to rely on. In addition, the study could incorporate and test the relationship between the perceived threat (its significance and likelihood), skills and competence of different individual users and the sense of agency, self-efficacy and motivation to protect themselves, for example with the consideration of well-established theories and models, e.g. Protection Motivation Theory by R.W. Rogers. A larger, more diverse sample would also allow for more reliable comparisons and provide a more comprehensive picture of how different demographic groups approach and employ cybersecurity measures and tools. Investigating specific behaviors, e.g. password management, multi-factor authentication, verifying the sources of information or contacts, checking reliability and security of networks, systems or regular updates of software or applications could offer insights into the gap existing between knowledge, awareness and practice. Moreover, understanding how individuals apply digital security measures and tools could help devise and implement targeted strategies to improve digital security competence and practical cybersecurity skills among e-consumers.

References

1. Adel, A. (2023). Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities. *Smart Cities 2023, 6,* pp. 2742-2782. https://doi.org/10.3390/smartcities6050124
2. Al Rusayyis, W., Bakry, S.H., Arafah, M.A. (2022). E-Services Cybersecurity Assessment Model. *International Journal of Smart Education and Urban Society, 13(1),* https://doi.org/10.4018/IJSEUS.300737
3. Alkis, A., Kose, T. (2022). Privacy concerns in consumer E-commerce activities and response to social media advertising: Empirical evidence from Europe. *Computers in Human Behavior*, *137*. https://doi.org/10.1016/j.chb.2022.107412

4. Almansoori, A., Al-Emran, M., Shaalan, K. (2023). Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. *Applied Science, 13,* 5700. https://doi.org/10.3390/app13095700.
5. Alrababah, H., Iqbal, H., Khan, M.A. (2024).The Effect of User Behavior in Online Banking on Cybersecurity Knowledge, *International Journal of Intelligent Systems*, https://doi.org/10.1155/int/9949510
6. Alwin, D.F. (1997). Feeling thermometers vs. 7-point scales. *Sociological Methods &Research, 25*(3), 318-351.
7. Alzahrani, A. (2020). Coronavirus Social Engineering Attacks: Issues and Recommendations. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *Vol. 11, No. 5*. https://doi.org/10.14569/ijacsa.2020.0110523
8. Ballagas, R., Borchers, J., Rohs, M., Sheridan, J.G. (2006). The Smart Phone: A Ubiquitous Input Device, *IEEE Pervasive Computing, Vol. 5, No. 1*, pp. 70-77.
9. Blessing, G., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., Pospelova, V. (2022). The Emerging Threat of AI-driven Cyber Attacks: A Review. *Applied Artificial Intelligenc*. https://doi.org/10.1080/08839514.2022.2037254
10. Boratyńska, K., Cieślik, E., Kacperska, E., Łukasiewicz, K., Milewska, A. (2021). *Gospodarka cyfrowa we współczesnym świecie – kraje V4.* Warsaw: SGGW.
11. Bylok, F. (2019). Wyzwania dla edukacji konsumenckiej w budowaniu świadomości konsumenckiej. In: M. Janoś-Kresło, M. (ed.), *Bezpieczeństwo konsumentów. Ochrona i edukacja konsumencka*. Warsaw: SGH.
12. Bytniewski, A. (ed.) (2013). *Systemy informatyczne a rozwój społeczeństwa informacyjnego*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.
13. Cele, N.N., Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, https://doi.org/10.1108/jfc-10-2023-0263
14. Chmielarz, W., Szumski, O. (2018). Cyber Security Patterns Students Behavior and Their Participation in Loyalty Programs. *International Journal of Ambient Computing and Intelligence. April 20189(2).* IGI Global Scientific Publishing, pp. 16-31, https://doi.org/10.4018/IJACI.2018040102
15. Churchill, G., Peter, P. (1984). Research design effects on the reliability of rating scales: A meta-analysis. *Journal of Marketing Research, 21*(4), pp. 360-375.
16. Cichosz, J. (2017). Społeczny wymiar problematyki bezpieczeństwa obywateli Unii Europejskiej w cyberprzestrzeni. Analiza porównawcza. In: J. Trubalska, Ł. Wojciechowski (Ed.), *Bezpieczeństwo osób w cyberprzestrzeni.* Lublin: Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie, 63-78.
17. Cox, E.P. (1980). The optimal number of response alternatives for a scale: A review. *Journal of Marketing Research, 17*(4), pp. 407-422.

18. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R. (2013). Future directions for behavioral information security research. *Computer Security*, *32*, pp. 90-101, https://doi.org/10.1016/j.cose.2012.09.010
19. Ćwiek, M., Maj-Serwatka, K. (2024). Digital Competence of Young Adults in Poland. *Folia Oeconomica. Acta Universitatis Lodziensis, 3(368)*, DOI: https://doi.org/10.18778/0208-6018.368.03
20. Dąbrowska, A., Fandrejewska, A., Stańczyk, E., Szalonka, K. (2025). *Consumer and Innovations in e-Health Services*. New York: Routledge, Taylor&Francis.
21. Dąbrowska, A., Bylok, F., Janoś-Kresło, M., Kiełczewski, D., Ozimek, I. (2015). *Kompetencje konsumentów. Innowacyjne zachowania, zrównoważona konsumpcja*. Warsaw: PWE.
22. Dudycz, H., Krawiec, Ł. (2018), Propozycja procedury badania użyteczności witryn internetowych, *Informatyka Ekonomiczna, No. 3(49)*, pp. 65-77.
23. European Commission: Directorate-General for Research and Innovation, MacCallum, D., Moulaert, F., Leubold, B., Mehmood, A. (2017). *Social innovation as a trigger for transformations – The role of research.* Publications Office, https://data.europa.eu/doi/10.2777/68949
24. Ewoh, P., Vartiainen, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research, 26*, https://doi.org/10.2196/46904
25. Fortes, N., Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*, *3,* 167-176. https://doi.org/10.1016/j.iedeen.2016.04.002
26. Gwoździewicz, S., Prokopowicz, D., Grzegorek, J. (2025). Chapter 4. Zastosowanie zaawansowanych narzędzi przetwarzania danych w dobie cyfryzacji. In: A. Laskowska-Rutkowska (ed.), *Cyfryzacja w zarządzaniu. Second edition*. Warsaw: CeDeWu.
27. Hossain, S.T., Yigitcanlar, T., Nguyen, K., Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences, No. 14, 5501*, https://doi.org/10.3390/app14135501
28. Jaciow, M., Wolny, R. (2011). *Polski e-konsument. Typologia, zachowania*. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.
29. Jaciow, M., Wolny, R., Stolecka-Makowska, A. (2015). *E-konsument w Europie. Komparatywna analiza zachowań*. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.
30. Jalali, M.S., Razak, S., Gordon, W., Perakslis, E., Madnick, S. (2019). Health Care and Cybersecurity: Bibliometric Analysis of the Literature. *Journal of Medical Internet Research, 21(2)*, https://doi.org/10.2196/12644
31. Janoś-Kresło, M. (ed.) (2019). *Bezpieczeństwo konsumentów. Ochrona i edukacja konsumencka*. Warsaw: Oficyna Wydawnicza SGH.

32. Kiran, U., Khan, N.F., Murtaza, H., Farooq, A., Pirkkalainen, H. (2025). Explanatory and predictive modeling of cybersecurity behaviors using protection motivation theory. *Computers & Security, 149*, https://doi.org/10.1016/j.cose.2024.104204.
33. Kotlorz, D. (2013). *Serwicyzacja polskiej gospodarki − przemiany wewnątrzsektorowe*. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.
34. Kozłowska, A. (2019). Chapter 8. Poszanowanie praw konsumenta: czy reklama może być uczciwa? In: M. Janoś-Kresło (ed.) (2019). *Bezpieczeństwo konsumentów. Ochrona i edukacja konsumencka*. Warsaw: Oficyna Wydawnicza SGH.
35. Lamond, M.L., Renaud, K.V., Wood, L.A., Prior, S. (2022). SOK: Young children's Cybersecurity Knowledge, Skills & Practice: A Systematic Literature Review. *EuroUSEC'22: proceedings of the 2022, European Symposium on Usable Security*, https://doi.org/10.1145/3549015.3554207
36. Laskowska-Rutkowska, A. (ed.) (2025). *Cyfryzacja w zarządzaniu. Second edition.* Warsaw: CeDeWu.
37. Mackey, T.K. Nayyar, G. (2016). Digital danger: a review of the global public health, patient safety and cybersecurity threats posed by illicit online pharmacies. *British Medical Bulletin, Vol. 118, Iss. 1*, 110-126, https://doi.org/10.1093/bmb/ldw016
38. Matell, M.S., Jacoby, J. (1971). Is there an optimal number of alternatives for Likert scale items? Study: Reliability and validity. *Educational and Psychological Measurement, 31*(3), 657-674.
39. Mocanu, F. (2013). Digital Literacy Among Young Adults in Romania. *Management Dynamics in the Knowledge Economy, Vol. 6, No. 3*, pp. 449-470; https://doi.org/10.25019/MDKE/6.3.06
40. Moustafa, A., Bello, A., Maurushat A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*. https://doi.org/10.3389/fpsyg.2021.561011
41. Mróz, B. (2020). Chapter 5. Prywatność i ekshibicjonizm w przestrzeni wirtualnej: implikacje dla bezpieczeństwa konsumentów. In: *Bezpieczeństwo konsumentów na rynku tradycyjnym i wirtualnym*. Warsaw: Oficyna SGH, pp. 65-76.
42. Mróz, B. (ed.) (2020). *Bezpieczeństwo konsumentów na rynku tradycyjnym i wirtualnym*. Warsaw: Oficyna SGH, pp. 25-36.
43. Mruk, H. (2020). Chapter 2. Pułapki behawioralne a zdrowie . In: B. Mróz (ed.) (2020). *Bezpieczeństwo konsumentów na rynku tradycyjnym i wirtualnym*. Warsaw: Oficyna SGH, pp. 25-36.
44. Nguyen, T.T., Tran, T.N.H., Do, T.H.M., Dinh, T.K.L., Nguyen, T.U.N. , Dang, T.M.K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, *10, 2,* https://doi.org/10.1016/j.joitmc.2024.100292

45. Nowacki, R., Fandrejewska, A. (2024). Nowacki Robert, Fandrejewska Alicja, Consumer Trust in Online Advertising - How Negative Perception Impacts its Effectiveness. *Current Social Sciences, Vol. 2*, https://doi.org/10.2174/012772316x276725240130110311
46. Nowacki, R., Fandrejewska, A. (2025). Next tech a prywatność danych i bezpieczeństwo użytkowników Internetu – perspektywa przedstawicieli pokolenia Z. In: M. Twardzik, L. Shulhina (eds.), *Bezpieczeństwo konsumenta na rynku nowych technologii i wybranych rynkach usług*. Warsaw: Oficyna Wydawnicza SGH.
47. Oh, S.S., Kim, K.A., Kim, Minsu, Oh, J., Chu, S.H., Choi, J. (2021). Measurement of Digital Literacy Among Older Adults: Systematic Review. *Journal of Medical Internet Research, Vol. 23, Iss. 2, e26145*, https://doi.org/10.2196/26145
48. Olak, R. (2024). *Badanie EY: Rosną obawy konsumentów o bezpieczeństwo ich danych.* 17 September 2024. https://www.ey.com/pl_pl/newsroom/2024/09/rosna-obawy-konsumentow-o-bezpieczenstwo-ich-danych
49. Papińska-Kacperek, J. (2013). Podaż i popyt na usługi cyfrowe w Polsce. In: A. Bytniewski, (ed.), *Systemy informatyczne a rozwój społeczeństwa informacyjnego*. Wrocław: Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.
50. *Postawy Polaków wobec cyberbezpieczeństwa 2024 – Wybrane dane z badania*. July 2024, https://cyber.wib.edu.pl/wp-content/uploads/2024/07/fragment-badania-Postawy-Polakow-wobec-cyberbezp._VII-2024.pdf
51. Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91(1),* pp. 93-114.
52. Sadab, M. (2023). *Key Factors Related to Cyber Security Affecting Consumer Attitude in Online Shopping - A Study in Bangladesh. MA thesis*. Faculty of Science and Technology, University of Canberra. https://researchsystem.canberra.edu.au/ws/portalfiles/portal/93581530/Mostofa_Sadab.pdf
53. Schutz, H.G., Rucker, M.H. (1975). A comparison of variable configurations across scale lengths: An empirical study. *Educational and Psychological Measurement, 35*(2), 319-324.
54. Singh, N., Misra, R., Quan, W., Radic, A., Lee, S.-M., Han, H. (2024). An analysis of consumer's trusting beliefs towards the use of e-commerce platforms. *Humanities and Social Sciences Communications, 11, 899*. https://doi.org/10.1057/s41599-024-03395-6.
55. Siponen, M., Rönkkö, M., Fufan, L., Haag S., Laatikainen, G. (2024). Protection motivation theory in information security behavior research: reconsidering the fundamentals. *Communications of the Association for Information Systems*, *53(1)*, pp. 1136-1165, https://doi.org/10.17705/1CAIS.05348.
56. Snopkiewicz, K. (2020). Przegląd zagrożeń w cyberprzestrzeni. *Studia Administracji i Bezpieczeństwa, Iss. 9*, pp. 29-41.
57. Stallings, W., Brown, L. (2019) *Bezpieczeństwo systemów informatycznych. Zasady i praktyka, Vol. 1*. Fourth edition. Pearson.

58. Tarka, P. (2015). Własności 5- i 7-stopniowej skali Likerta w kontekście normalizacji zmiennych Metodą Kaufmana i Rousseeuwa [Properties of the 5- and 7-point Likert scale in the context of variable normalization using the Kaufman and Rousseeuw method]. *Research Papers of Wrocław University of Economics, 385*, 286-295. https://doi.org/10.15611/pn.2015.385.31
59. Trubalska, J. Wojciechowski, Ł. (ed.) (2017). *Bezpieczeństwo osób w cyberprzestrzeni*. Lublin: Innovatio Press Wydawnictwo Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie, pp. 63-78.
60. Wahab, F., Khan, I., Kamontip, Hussain, T., Amir, A. (2023). An investigation of cyber attack impact on consumers' intention to purchase online. *Decision Analytics Journal*, *8*. https://doi.org/10.1016/j.dajour.2023.100297.
61. Wasilewski, J. (2013). Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego, 9*, pp. 225-234.
62. Wilk, A. (2013). *Kradzież tożsamości. Raport z Badań.* FELLOWERS, 3.10.2013, p. 25.
63. Wisetpanich, N., Wittayakom, S., Warrarith, S., Jadesadalug, V. (2025). Canonical Correlation Analysis of Digital Literacy and Perceived Data Privacy Security in E-Commerce Platform Usage Among Generation Z in Thailand. *Pakistan Journal of Life and Social Sciences, 23(1).*
64. Wolny, R. (2013). *Rynek e-usług w Polsce – funkcjonowanie i kierunki rozwoju*. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.
65. Wolny, R. (2020). Rozdział 7. Świadomość istnienia niebezpieczeństw korzystania z e-usług wśród młodych konsumentów. In: B. Mróz (ed.) (2020). *Bezpieczeństwo konsumentów na rynku tradycyjnym i wirtualnym.* Warsaw: Oficyna Wydawnicza SGH, pp. 89-100.
66. Zhang, M., Kaur, M. (2024). Toward a theory of e-government: Challenges and opportunities, a literature review. *Journal of Infrastructure Policy and Development*, *8(10),* 7707. https://doi.org/10.24294/jipd.v8i10.7707
67. Ziemba, E. (2017). *Zrównoważone społeczeństwo informacyjne*. Katowice: Wydawnictwo Uniwersytetu Ekonomicznego w Katowicach.