

SENIORS' SENSE OF DIGITAL SECURITY AND THEIR ACTIVITY IN USING INTERNET SERVICES

Michał DZIADKIEWICZ^{1*}, Paulina BANASIK²

¹ Czestochowa University of Technology, Faculty of Management; michal.dziadkiewicz@pcz.pl,
ORCID: 0000-0001-5450-1669

² Czestochowa University of Technology, Faculty of Management; paulina.banasik@pcz.pl,
ORCID: 0009-0001-2855-262X

* Correspondence author

Purpose: The purpose of the article is to analyse the relationship between the awareness and sense of digital security of seniors and their activity in using Internet services in the context of information security management.

Design/methodology/approach: The study used quantitative analysis of data collected using the PAPI technique on a sample of 220 people aged 60+. The research tool was a questionnaire containing questions about digital literacy, frequency of internet use, sense of security and experiences of threats.

Findings: The results indicate that seniors are active Internet users, but their participation in the digital environment is diverse. Higher self-assessment of digital competence is associated with more frequent internet use, while a lower sense of security and fear of fraud limit one's online activity. The respondents also report high awareness of the most common online threats.

Research limitations/implications: The study included 220 seniors from Poland, which limits the possibility of full generalization of the results. The sample was diverse but not fully representative, especially in terms of regional structure. Further research should include a larger and more balanced sample and consider variations in digital competences by age, place of residence, and professional experience.

Practical implications: The results can support the design of educational activities aimed at seniors and the creation of simpler and safer digital solutions. They also have implications for public institutions, banks, and online service providers, which should consider the needs of older users.

Originality/value: This article combines the perspectives of digital literacy, sense of security, and information security management, focusing on seniors as a group that is particularly vulnerable to online threats.

Keywords: seniors; digital competence/skills/literacy; information security; Internet; digital exclusion.

Category of the paper: Research paper.

1. Introduction

Poland, like other European Union member states, has been facing a growing demographic challenge for many years, which is the systematic increase in the percentage of older people in the structure of society. This phenomenon generates significant consequences for the functioning of the social system, the labour market, health care and public policy, and also places new requirements on the adaptation processes related to the ongoing digitalization (Hargittai, Dobransky, 2017; van Deursen, Helsper, 2015). In this context, the issue of digital integration of people over 60, understood as the possibility of their full and safe participation in the information and service environment of modern society, is of particular importance. This problem was already noticed at the strategic level, which was reflected in the inclusion of the activation of older people in the Lisbon Strategy adopted by the European Council in 2000. This document emphasized, among other things, the need to support the employment of older people through training and competence-building activities, which was to help them stay longer in the labour market.

The ongoing digitalization of social and economic life has led to the fact that using the Internet is no longer just an additional option but has become a condition for effective functioning in many areas of everyday life (Park, Nam, Cha, 2021; Xie, 2025). This applies to contact with public institutions, the implementation of financial operations, access to information, and maintaining social relations. For older people, this means not only mastering basic technical skills but also developing competences that allow for critical evaluation of content, recognition of risks, and also conscious and responsible use of digital services (Maciąg, 2021; Olphert, Damodaran, 2013). At the same time, the intensive development of communication technologies contributes to the increase in the number of threats in cyberspace, such as phishing, identity theft, online fraud and personal data theft, which further complicates the situation of users with a lower level of digital competences (Crossler, Belanger, 2014; Whitman, Mattord, 2021).

Seniors are a group that is particularly vulnerable to digital exclusion, which should be understood not only as a lack of access to technologies, but also as a limitation of their effective, safe and autonomous use (Hargittai, Dobransky, 2017; van Deursen, Helsper, 2015). This exclusion is multidimensional and may result from hardware, economic, cognitive, psychological and social barriers. In practice, this means that some older people, despite the formal availability of the Internet and electronic services, are not able to fully use them due to insufficient competences, fear of making a mistake, low level of trust in technology or negative experiences related to their use (Olphert, Damodaran, 2013; van Dijk, 2020). Such restrictions lead to enhancement of social inequalities because they exclude seniors from important areas of public life. Importantly, a lack of competence in information security may reinforce concerns about using the Internet and thus lead to abandonment of digital services even when they are

potentially useful. As a result, both the actual level of knowledge about threats and the subjective sense of digital security may significantly influence the scope of seniors' activity in the online environment (Bulgurcu et al., 2010; Hargittai, Dobransky, 2017).

The purpose of the article is to analyse the relationship between the awareness and sense of digital security of seniors and their activity in using Internet services in the context of information security management.

2. Literature review

2.1. Information security management

Services such as online banking, e-government, medical platforms and instant messengers provide convenience and increase access to information and services, but at the same time require an appropriate level of digital competences and the ability to identify threats (Whitman, Mattord, 2021). In the case of older people, these skills may be limited by less technological experience, lower self-confidence in using digital tools and greater susceptibility to manipulation (Maciąg, 2021).

Information security management should therefore not be understood solely as a set of technical data protection measures, but as a comprehensive process that also covers the end user, their knowledge, behaviour and level of threat awareness (Crossler, Belanger, 2014; Siponen, Oinas-Kukkonen, 2007). The effectiveness of security systems depends not only on the infrastructure security measures used, but also on organizational and human factors, including the ability to recognize social engineering attacks, the use of secure passwords, and the careful use of electronic messages and links sent online (Siponen, Oinas-Kukkonen, 2007). In the case of seniors, the importance of these elements is particularly high, as cybercriminals often take advantage of the limited vigilance of this group by impersonating public institutions, banks or family members.

Therefore, the literature emphasizes the need to develop educational activities aimed at seniors, which should be adapted to their cognitive and practical needs (Olphert, Damodaran, 2013). Effective support programs cannot be limited to providing theoretical knowledge, but should include practical exercises, simple language of communication and the possibility of individual support in problem situations (Mick, Fournier, 1998; Olphert, Damodaran, 2013). Research shows that a digital safety training increases one's awareness of threats, strengthens the sense of empowerment and promotes more conscious use of the Internet by older people (Mick, Fournier, 1998; Olphert, Damodaran, 2013). In this way, educational activities become one of the key elements of information security management for this group of users.

From an organizational perspective, this means that public institutions, financial entities and digital service providers should design solutions that take into account the needs of seniors. This applies to both IT system interfaces and security procedures, which should be clear, intuitive and possible to use independently (Bulgurcu et al., 2010). The literature indicates that excessive complexity of security procedures may paradoxically reduce their effectiveness, because users – especially older ones – refrain from using them or perform them incompletely (Bulgurcu et al., 2010). Therefore, effective information security management should combine technical protection with ease of use and educational support.

Including seniors in the analysis of information security management also allows for a better understanding of the social consequences of digitalization. Older people who do not feel safe in the online environment are more likely to limit the use of e-services, which leads to an enhanced digital exclusion and a reduction in their participation in social life. Therefore, information security should be considered not only as a matter of data protection, but also as a condition for digital inclusiveness, enabling all social groups to fully and safely participate in the information society (Helsper, 2012; van Dijk, 2020).

2.2. Digital literacy of seniors

With the increasing digitalization of social, economic and administrative life, the ability to use information and communication technologies has become an essential element of everyday functioning (van Dijk, 2020; European Commission, 2022).

Digital literacy can be understood as a set of knowledge, skills and attitudes that enable effective, critical, safe and responsible use of digital technologies. These include not only the basic operation of devices and applications, but also the ability to search, select and evaluate information, communicate via digital tools, solve technical problems and protect personal data and privacy in the online environment (European Commission, 2022).

In the case of seniors, digital competences play a particularly important compensatory and integrative role (van Dijk, 2020). On the one hand, they help eliminate barriers related to limited mobility, lower availability of stationary services and difficulties in direct social contact. On the other hand, they enable the use of an increasing number of services transferred to the digital space. Research shows that the level of digital skills affects the quality of life of older people because it strengthens their independence, facilitates access to health and social information and supports maintaining interpersonal relationships (Xie, 2025). In this sense, digital competences are not only a technical tool, but also a social and psychological resource.

However, the level of digital literacy of seniors varies and depends on many factors, such as education, financial situation, place of residence, health condition, previous professional experience and social environment (Hargittai, Dobransky, 2017; van Deursen, Helsper, 2015). Older people living in large cities, with higher education or previous professional experience related to technology, often demonstrate higher levels of digital literacy than seniors from rural areas or those who have not used computer tools before

(van Deursen, Helsper, 2015; Hargittai, Dobransky, 2017). In Polish conditions, the level of digital competences of older people still remains diverse, and some of them have difficulties in using digital devices and services independently, which increases the risk of information and social exclusion (UKSW, 2023).

In practice, many seniors have only basic digital skills, limited to using a mobile phone, browsing websites or sending messages. More advanced activities, such as using public e-services, online shopping, e-banking, configuring privacy settings or recognizing digital threats, may pose a significant challenge for them (van Deursen, Helsper, 2015). As a result, some older people use the Internet selectively and cautiously, focusing only on the simplest functions that they consider safe and understandable (Maciąg, 2021; Olphert, Damodaran, 2013).

The development of digital skills among seniors faces a number of barriers. One of the most frequently mentioned one is the fear of making a mistake and the negative consequences of using technology (Hargittai, Dobransky, 2017; van Deursen, Helsper, 2015). Older people may be afraid of data loss, financial fraud, installing malware or making irreversible changes to their device. Another obstacle is the low self-esteem of one's own competences, which may lead to giving up on trying to learn new solutions on one's own (Hargittai, Dobransky, 2017). The literature also highlights the importance of complexity of digital interfaces and procedures, which are often not designed with the needs of older users in mind. Excessive complexity of systems may reduce the effectiveness of their use and reinforce the feeling of exclusion (van Deursen, Helsper, 2015; Hargittai, Dobransky, 2017).

An important dimension of seniors' digital literacy is also the safety of using the Internet. The ability to recognize reliable sources, assess the authenticity of messages, use strong passwords, protect personal data and identify phishing attempts is now one of the basic elements of digital independence (Bulgurcu et al., 2010). Lack of competence in this area may lead to particular vulnerability to manipulation and online fraud. As the literature on user behaviour indicates, effective use of technology requires not only technical knowledge, but also awareness of risks and a willingness to apply the principles of safe use (Bulgurcu et al., 2010). In the case of seniors, this is particularly important because they are often the targets of attacks using social engineering, fake news and attempts to impersonate public or financial institutions (ENISA, 2025).

2.3. Threats in the digital environment

The development of information and communication technologies has brought numerous benefits, but at the same time it has created new areas of risk. The digital environment, understood as a set of services, devices, platforms and communication channels based on Internet technologies, has become an area of intense user activity and, at the same time, a field of action for cybercriminals (ENISA, 2024; Whitman, Mattord, 2021). The literature emphasizes that digital threats are not limited to technical problems, but also include social,

psychological and organizational aspects, affecting users' trust, behaviour and level of participation in online life (Whitman, Mattord, 2021).

Modern threats in the digital environment are multidimensional and dynamic. They include, among other things, phishing, identity theft, financial fraud, malware, fake websites, social engineering manipulation, data leaks, and various types of attacks on user accounts (NASK, 2024; ENISA, 2024). From the perspective of information security, it is particularly important that many of these threats exploit not so much technical loopholes as human weaknesses, such as haste, lack of vigilance, trust in messages or difficulty in recognizing inauthentic content. Therefore, effective protection against digital threats requires not only technical security measures, but also appropriately developed user competences and risk awareness (Bulgurcu et al., 2010; Siponen, Oinas-Kukkonen, 2007).

Financial fraud is also a significant threat area. With the widespread use of online and mobile banking, cybercriminals are increasingly focusing on gaining access to bank accounts, payment card details, and transfer authorizations (PAP, 2024; NASK, 2024). Seniors who use online payments may be exposed to fake banking websites, dishonest online stores, impersonations of bank consultants or attempts to obtain authorization codes. According to expert reports, older people are a frequent target of this type of activities, and the scale of financial fraud attempts against this group remains significant (PAP, 2024; Bank Pocztowy, 2026).

The risks associated with privacy violations and personal data leakage cannot be ignored either. In the digital environment, users leave behind numerous information traces that can be collected, analysed and used in a way that is against their will. For seniors, who are not always aware of the scale of data processing, this is a serious challenge. Lack of knowledge about privacy settings, cookie policies, or online tracking mechanisms can lead to unintentional sharing of personal information. From a data protection perspective, this issue is particularly important because privacy violations can be the starting point for further criminal activities, including identity theft, harassment or advertising manipulation (Whitman, Mattord, 2021).

Preventive and educational efforts are crucial. Research and institutional studies indicate that increased digital literacy among seniors translates into greater resistance to fraud and more conscious use of online services (PAP, 2024; NASK, 2024). This includes such abilities as recognizing suspicious messages, using strong passwords, using multi-factor authentication, checking website addresses, and being wary of unexpected requests for data or money (NASK, 2024; ENISA, 2024).

3. Research methodology

The purpose of the study was to identify the relationship between the level of awareness and sense of digital security of seniors and their activity in using Internet services, taking into account issues related to information security management. In order to achieve the research objective, two hypotheses were formulated:

H1. A higher level of digital competence among seniors promotes more frequent use of the Internet and electronic services.

H2. The level of awareness of threats and the sense of digital security are significantly related to the activity of seniors in using internet services.

The study was carried out as part of the project "Together for the safety of seniors" using the PAPI technique, i.e. a direct questionnaire interview conducted using a paper form. The questionnaire consisted of 13 main questions divided into four thematic sections covering demographic characteristics, digital literacy, sense of digital security and the use of electronic services. The first part included questions concerning gender, education, place of residence and source of income. The second section focused on the respondents' level of digital literacy and frequency of Internet use, while the third part concerned perceived online threats, sense of digital security and experiences related to fraud attempts in the digital environment. The final section referred to the use of selected electronic services, including online banking, communication platforms and public e-services. Most of the questions were closed-ended and based on ordinal response scales allowing respondents to assess the frequency of Internet use, level of digital competences and perceived online security. Several questions allowed respondents to indicate more than one answer, especially in the part concerning the identification of online threats and previous experiences with fraud attempts. The research tool also allowed us to identify respondents' attitudes towards cyber threats.

The research group consisted of elderly people over 60 years of age who lived in Poland. A total of 220 respondents participated in the study. The collected data was analysed quantitatively, and the results were converted to percentages, which were then rounded to one decimal place.

The structure of the research sample was diversified in terms of sociodemographic characteristics, which allows for a multidimensional characterization of the studied population.

Women clearly predominated among the respondents, constituting 72.2% of all subjects, while the percentage of men was 27.8%. In terms of education level, the largest category were people with secondary education, who accounted for 49% of the sample. The subsequent places were occupied by people with higher and vocational education, while people with primary education constituted only 0.9% of the respondents. In terms of place of residence, respondents living in urban communes (municipalities) were the dominant group, constituting 83.6% of the sample. The share of residents of rural communes and urban-rural communes was much

smaller. The analysis of the source of income shows that more than half of the respondents were retirees and pensioners (53.4%), and the next large group were salaried employees (36.1%). Other sources of income, such as own business, contract of mandate, occasional work, agriculture, unemployment or other forms of income, were marginal. This means that the sample was largely dominated by people outside the full, active labour market. The structure of the studied sample is presented in detail in Table 1.

Table 1.
Characteristics of the study sample

Variable	Category	% of responses
Gender	Male	27.8
	Female	72.2
Education	Primary	0.9
	Vocational	14.1
	Secondary	49
	Higher	35.9
Place of residence	Urban commune	83.6
	Urban-rural commune	6.1
	Rural commune	10.3
Source of income	Salaried employment	36.1
	Agriculture	0.5
	Own business	3.7
	Contract of mandate	3.2
	Retiree/pensioner	53.4
	Occasional work	0.9
	Unemployed	1.4
	Other	0.9

Source: Own study.

The structure of the research sample indicates that the study covered mainly socially active and relatively well-educated people, which may contribute to a higher level of orientation in the digital environment. At the same time, the significant share of retirees and pensioners confirms that the sample largely reflects the senior population to which the analysed results refer. This profile of respondents provides an important background for further analysis of their digital competences, Internet use and perceived online security.

4. Research results

4.1. Digital literacy and Internet use

The first part of the results analysis focused on the digital competences of the surveyed seniors and the frequency of their Internet use. The comparison of answers to questions about self-assessment of Internet skills and the intensity of Internet use allows us to determine the general level of digital engagement of respondents and provides a starting point for further considerations regarding their online activity.

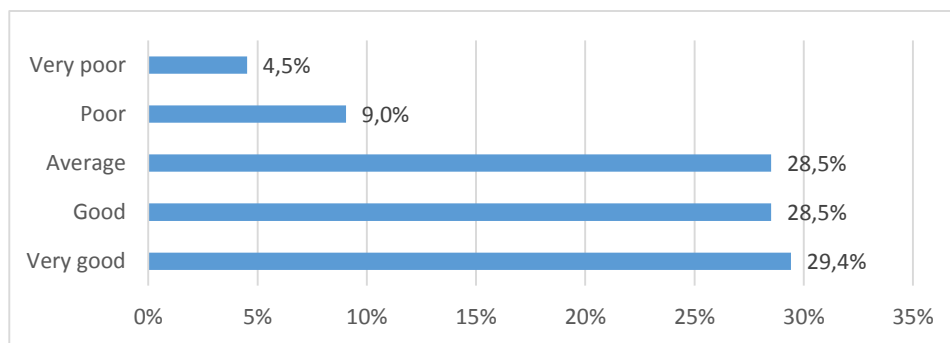


Figure 1. Respondents' answers to the question related to the assessment of their Internet use skills – "How do you assess your Internet use skills?".

Source: own study.

The analysis of responses to the question regarding self-assessment of Internet use skills indicates that the surveyed seniors most often described their digital competences as very good (29.4%) or good (28.5%). A similar percentage of respondents rated them as average (28.5%), while a smaller group provided such responses as poor (9.0%) and very poor (4.5%).

These results suggest that the older people included in the study do not remain completely outside the digital sphere, but participate in the online space to varying degrees. At the same time, a noticeable percentage of "average" and "poor" responses shows that some respondents may still experience difficulties in using the Internet independently and confidently. In the context of further analyses, it will be important to determine whether the subjective assessment of competences translates into the actual level of digital activity.

It should be noted, however, that the declared activity does not necessarily mean full independence or high digital agency. Some older people may use the Internet selectively, limiting it to the simplest functions, avoiding more complex services that require logging in, authorization, or making financial decisions. This phenomenon fits well into the broader concept of digital exclusion, understood not only as a lack of access to technology, but also as a limited level of its effective and safe use. In this sense, the mere presence of seniors in the digital environment does not mean their full integration into digital society.

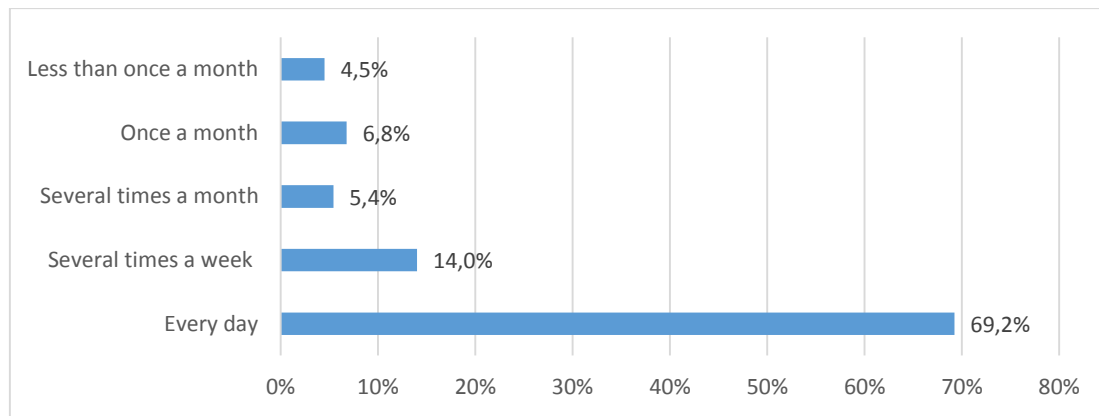


Figure 2. Respondents' answers to the question about the frequency of Internet use – "How often do you use the Internet?".

Source: own study.

The answers to the question about the frequency of Internet use confirm that the Internet is an important element of everyday functioning for most respondents. The largest group of respondents declared using the Internet every day (69.2%), and the next one – several times a week (14.0%). Smaller percentages indicated using the Internet once a month (6.8%), several times a month (5.4%) and less than once a month (4.5%).

Based on the distribution of answers to both questions, it can be concluded that there is a clear tendency for higher self-assessment of digital competences to coexist with more frequent use of the Internet. Among people who assessed their digital literacy as good or very good, daily use of the Internet was dominant, which suggests that higher self-assessment of skills is associated with greater intensity of online activity. In turn, those respondents who assessed their competences as average or poor more often declared less frequent use of the Internet, which may indicate limited confidence in navigating the digital environment. The obtained results can be interpreted as confirmation of hypothesis H1, according to which a higher level of digital competences among seniors promotes more frequent use of the Internet and electronic services.

4.2. Sense of security and experience of threats on the Internet

An important element of the analysis was also the sense of security and the respondents' experiences related to threats and frauds while using the Internet, which was verified by subsequent questions.

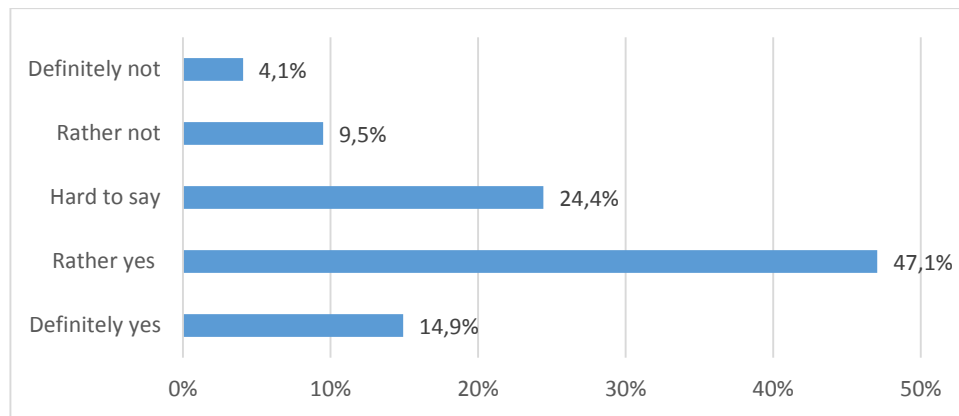


Figure 3. Respondents' answers to the question about their sense of security on the Internet – "Do you feel safe when using the Internet?".

Source: own study.

The results indicate that most seniors declare a relatively good sense of security when using the Internet, but this does not mean full trust in the digital environment. Only 14.9% of subjects responded that they felt definitely safe on the Internet, and 47.1% indicated the answer "rather yes". In total, this gives 61.99% of the surveyed group who declare a positive sense of security. At the same time, 24.43% chose the answer "hard to say", 9.5% "rather not", and 4.1% "definitely not", which shows that for a significant part of the respondents, digital security is not an obvious and unambiguous category.

On this basis, it can be concluded that the level of digital security among seniors is moderate. On the one hand, positive answers predominate, suggesting familiarity with the Internet and some skill in using it, while the share of uncertain and negative answers shows that many seniors use the Internet with some caution. The feeling of security depends not only on the use of the Internet itself, but also on the level of knowledge about threats, personal and social experiences and the level of trust in technology.

This conclusion is further supported by the responses regarding the perception of Internet threats presented in Figure 4.

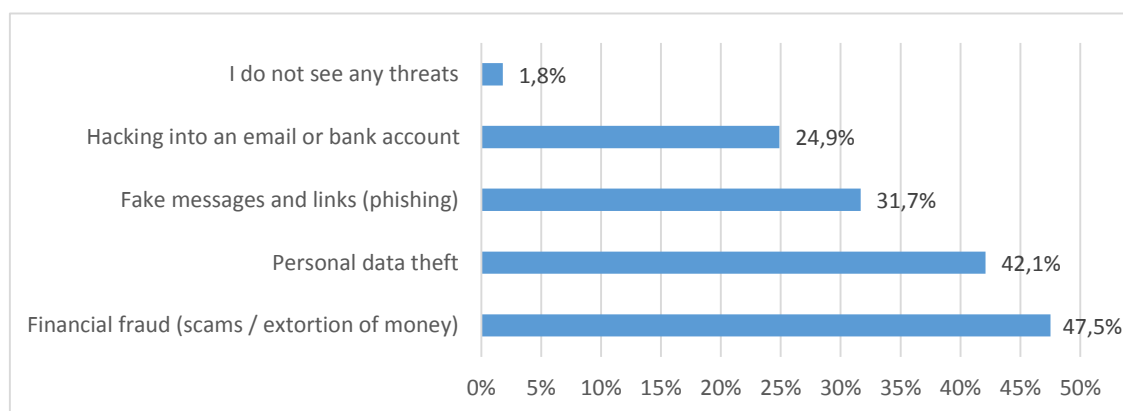


Figure 4. Respondents' answers to the question about the most significant threats on the Internet.

Source: own study.

The largest number of people, 47.5%, cited financial fraud. Second place went to personal data theft, selected by 42.1% of respondents, and third place went to phishing, which is fake messages and links, selected by 31.7% of respondents. This pattern of responses shows that seniors not only use the Internet, but are also able to recognize the most typical forms of cyber threats. The awareness of threats is also confirmed by the responses regarding the experience of fraud attempts presented in Figure 5. 35.3% of the respondents declared personal contact with an attempted online fraud, and 31.2% had heard about such cases. This means that more than half of the respondents had direct or indirect contact with attempted digital abuse. Such experiences may increase caution, but also lead to reduced trust in e-services.

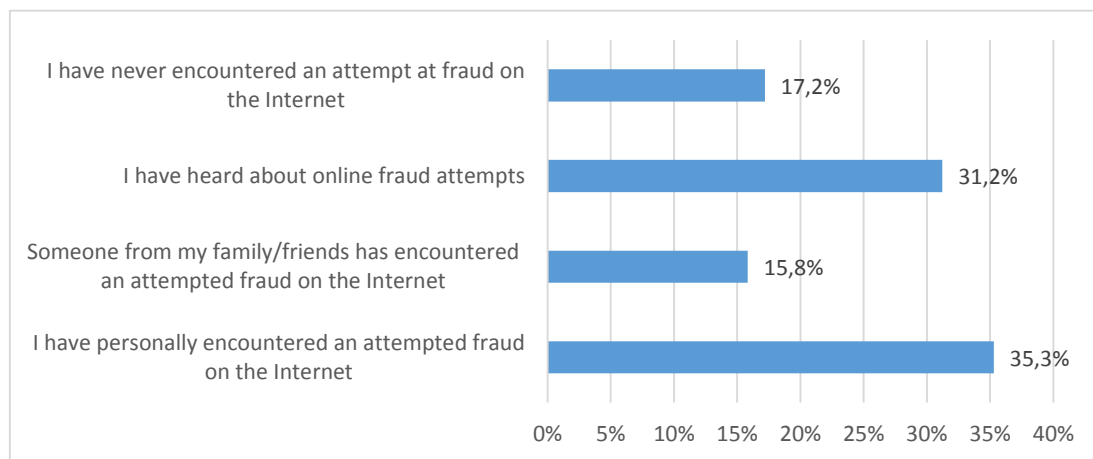


Figure 5. Answers to the question whether the respondent has ever encountered an attempted online fraud – “Have you ever encountered an attempted online fraud?”.

Source: own study.

Based on these results, it is clear that seniors are aware of real digital threats, but they do not always have the tools that would allow them to use them effectively and calmly. Such results show that the respondents are aware that using it is associated with a real risk. It is this awareness that may reduce the subjective sense of security, even when using the Internet is regular and efficient.

From the perspective of information security management, it is important that threat awareness can serve a dual purpose. On the one hand, it strengthens caution and encourages more responsible behaviour, but on the other hand, when combined with a low sense of competence, it can lead to anxiety and avoidance of technology. An older person who knows about online scams but does not feel confident enough in using technology may limit their contact with digital services out of fear of financial loss or loss of privacy. As a result, awareness of threats does not always translate into greater activity, but may coexist with a cautious attitude and partial withdrawal.

4.3. Demographic differences in digital activity and security perception

Although aggregate findings provide a useful general overview, a more detailed analysis indicates that older adults do not constitute a uniform group in terms of digital competencies and perceptions of online safety.

A tabulation of gender and self-assessed internet literacy (Figure 1) reveals notable differences in perceived digital proficiency and navigation styles. Although the frequency of daily internet use is comparably high in both groups, male respondents tend to report higher confidence in their digital skills. 34.4% of men rated their competencies as either “very good” or “good”. By contrast, female respondents demonstrated a more cautious self-evaluation, with only 27.5% placing themselves in the highest categories, while a larger proportion identified their skills as “average” (41.2%) or “poor/very poor”.

Gender also appears to shape the prioritisation of perceived online threats (Figure 4). While financial fraud (including scams and monetary extortion) constitutes the most frequently cited concern across the entire sample (47.5%), women show greater sensitivity to risks related to personal data and identity protection (44.3% among women versus 36.1% among men). These patterns are summarised in Table 2.

Table 2.

Gender-based differences in digital competencies, online threat perception, and sense of security among senior respondents

Category	Skill: very good / good	Skill: average	Threat focus: financial fraud	Threat focus: data theft	Sense of security: safe (yes)
Female	27.5%	41.2%	46.2%	44.3%	59.8%
Male	34.4%	32.8%	50.8%	36.1%	65.6%

Source: Own study.

Educational attainment represents a key structural factor shaping both levels of digital engagement and cybersecurity literacy within the surveyed older population. Respondents with a university degree demonstrate the highest levels of confidence in the digital environment, with 41,5% assessing their competencies as “very good” or “good”. Importantly, educational attainment not only influences self-perceived digital skills but also contributes to a more nuanced understanding of cybersecurity mechanisms. While individuals with vocational or primary education tend to focus predominantly on basic financial scams, university-educated seniors exhibit a more sophisticated awareness of structural threats, such as phishing attacks and malicious electronic communications (38.4% awareness within this subgroup). This is presented in table 3.

Table 3.

Educational differences in digital competencies, phishing awareness, and perceived online security among senior respondents

Education level	Skill: very good / good	Threat focus: phishing awareness	Sense of security: safe (Yes)	Sense of security: unsafe / hard to say
Vocational	16.1%	19.4%	48.4%	51.6%
Secondary	26.7%	29.5%	61.3%	38.7%
Higher	41.5%	38.4%	69.6%	30.4%

Source: Own study.

Older adults from rural areas, although still active internet users, report less frequent daily internet use and demonstrate a notably lower sense of digital safety (Figure 3). In this group, the combined share of negative or uncertain responses (“hard to say” or “rather unsafe”) reached 43.5%, compared to only 31.2% in urban municipalities. Seniors living in cities benefit from denser social networks, easier access to digital literacy initiatives (e.g., Universities of the Third Age), and more frequent exposure to smart-city solutions (e-banking, e-government services, online public transport systems). As a result, their sense of digital security is reinforced through continuous, supported engagement with technology, whereas rural seniors operate in an environment with more limited institutional support, which increases their perceived vulnerability to cyber threats.

5. Summary and conclusions

The analysis of the study results allows us to conclude that the surveyed seniors are present in the digital space to a significant extent, but their participation is diverse and heterogeneous. The Internet is an important tool for their everyday functioning, which is confirmed by both the high frequency of using the Internet and the relatively positive self-assessment of digital competences. At the same time, the obtained results indicate that this activity does not mean full freedom or complete confidence in using Internet services. Some of the respondents still declare an average or lower level of skills, as well as limited independence in using more advanced digital functions.

An important result of the analysis is the high level of awareness of Internet threats in the surveyed group. The subjects are able to recognize the most common online threats, including financial fraud, personal data theft and phishing. At the same time, a significant number of respondents have encountered fraud attempts directly or indirectly, which further increases their caution towards online services. As a result, the fear of fraud is becoming one of the most important factors limiting the fuller use of digital resources. This means that awareness of

threats does not only have a protective function, but can also lead to distancing oneself from technology and giving up more advanced online activities.

The purpose of the study was to determine the level of digital competences of seniors, their activity in using the Internet and the relationship between awareness of threats and the sense of digital security. The analysis of the results allowed us to achieve this objective, as it revealed both the scale of everyday use of the Internet and the perception of threats, experiences of fraud and limitations related to online services. The study showed that seniors are active Internet users, but their functioning in the digital space is largely dependent on trust, security and previous experience.

The obtained results allow us to consider hypothesis H1 as confirmed. A higher level of digital competence among seniors is associated with more frequent use of the Internet and electronic services. The respondents who assessed their own skills better were more likely to declare regular online activity and greater willingness to use digital tools. Hypothesis H2 is also confirmed by the study results. The level of awareness of threats and the sense of digital security remain significantly related to the activity of seniors in using Internet services. People who are better at recognizing threats and declare a higher level of security are more likely to use e-services, while a lower sense of security fosters a cautious attitude and limits digital activity.

The obtained results allow us to conclude that the activity of seniors in using Internet services remains strongly linked to the level of their digital literacy, awareness of threats and sense of security. Seniors are not a passive group in the face of digitalization - many of them use the Internet regularly and use electronic services in their daily lives. At the same time, however, the presence of concerns, lack of full certainty and technical difficulties indicate that the process of their digital integration has not yet been completed.

The results obtained in this study are consistent with findings presented in previous literature concerning digital literacy and online security among older adults. Similar relationships between digital competences and the intensity of Internet use were identified by van Deursen and Helsper (2015), who emphasized that higher digital skills increase both the frequency and diversity of online activities among seniors. Comparable conclusions were also presented by Hargittai and Dobransky (2017), who demonstrated that digital inequalities among older adults are strongly associated with education level, previous technological experience and self-confidence in using digital tools.

The present study also confirms observations described by Olphert and Damodaran (2013), according to which awareness of online threats may simultaneously increase caution and reduce willingness to engage in more advanced digital activities. Similar conclusions regarding the importance of digital security awareness for safe online participation were formulated in reports by ENISA (2024) and NASK (2024), which highlighted that seniors remain one of the groups particularly vulnerable to phishing, financial fraud and social engineering attacks.

Therefore, the obtained findings support the broader conclusion present in the literature that effective digital inclusion of seniors requires not only access to technology, but also continuous educational support, development of digital competences and strengthening users' sense of online security.

References

1. Bank Pocztowy (2026). *46% Polaków miało styczność z próbą oszustwa internetowego, seniorzy coraz ostrożniejsi*. Retrieved from: <https://prnews.pl/46-polakow-mialo-stycznosc-z-proba-oszustwa-internetowego-seniorzy-coraz-ostrozniejsi-489117>, 05.05.2026.
2. Bulgurcu, B., Cavusoglu, H., Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, Vol. 34, Iss. 3, pp. 523-548.
3. Crossler, R., Belanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database*, Vol. 45, Iss. 1, pp. 51-71, doi: 10.1145/2691517.2691521.
4. European Commission (2022). *Digital competence framework for citizens (DigComp 2.2): With new examples of knowledge, skills and attitudes*. Luxembourg: Publications Office of the European Union.
5. European Union Agency for Cybersecurity (2024). *ENISA threat landscape 2024*. Retrieved from: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>, 05.05.2026.
6. e.org.pl (2021). *Potrzeby i kompetencje medialne osób 55+*. Retrieved from: https://e.org.pl/wp-content/uploads/2021/11/Raport_Potrzeby-i-kompetencje-medialne-osob-55-plus.pdf, 05.05.2026.
7. gov.pl (2024). *Jak pokonać wykluczenie cyfrowe seniorów – okrągły stół w KPRM*. Retrieved from: <https://www.gov.pl/web/cyfryzacja/jak-pokonac-wykluczenie-cyfrowe-seniorow-okragly-stol-w-kprm>, 05.05.2026.
8. Hargittai, E., Dobransky, K. (2017). Old dogs, new clicks: Digital inequality in skills and uses among older adults. *Canadian Journal of Communication*, Vol. 42, Iss. 2, pp. 195-212.
9. Helsper, E.J. (2012). A corresponding fields model for the links between social and digital exclusion. *Communication Theory*, Vol. 22, Iss. 4, pp. 403-426, doi: 10.1111/j.1468-2885.2012.01416.x
10. ISO/IEC 27001:2022 (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva: International Organization for Standardization.

11. Maciąg, A. (2021). *Seniorzy jako użytkownicy nowych technologii informacyjno-komunikacyjnych*. Retrieved from: <https://rob.uksw.edu.pl/wp-content/uploads/2023/12/ekspertyza-04-21-12.pdf>, 05.05.2026.
12. Mick, D.G., Fournier, S. (1998). Paradoxes of technology: Consumer cognizance, emotions, and coping strategies. *Journal of Consumer Research*, Vol. 25, Iss. 2, pp. 123-143, doi: 10.1086/209531.
13. NASK (2024). *Analiza bezpieczeństwa polskiego internetu w 2024 roku*. Retrieved from: <https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku>, 05.05.2026.
14. NASK (2024). *Cyfrowy świat bez barier pokoleniowych*. Retrieved from: <https://www.nask.pl/aktualnosci/cyfrowy-swiat-bez-barier-pokoleniowych>, 05.05.2026.
15. NASK (2024). *Raport roczny z działalności CERT Polska w 2024 roku*. Retrieved from: <https://www.nask.pl/magazyn/raport-roczny-z-dzialalnosci-cert-polska-w-2024-roku>, 05.05.2026.
16. Olphert, W., Damodaran, L. (2013). Older People and Digital Disengagement: A Fourth Digital Divide? *Gerontology*, Vol. 59, Iss. 6, pp. 564-570, doi: 10.1159/000353630
17. Park, S., Nam, Y., Cha, C. (2021). Measurement of digital literacy among older adults: Systematic review. *JMIR Aging*, Vol. 4, Iss. 1, No. e26145, doi: 10.2196/26145
18. PAP (2024). *Wzrost kompetencji cyfrowych to większa odporność seniorów na oszustwa*. Retrieved from: <https://zdrowie.pap.pl/senior/wzrost-kompetencji-cyfrowych-wieksza-odpornosc-seniorow-na-oszustwa>, 05.05.2026.
19. Siponen, M., Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, Vol. 38, Iss. 1, pp. 60-80.
20. Stallings, W., Brown, L. (2018). *Computer security: Principles and practice* (4th ed.). Boston: Pearson.
21. UKSW (2023). *Seniorzy jako użytkownicy nowych technologii informacyjno-komunikacyjnych*. Retrieved from: <https://rob.uksw.edu.pl/wp-content/uploads/2023/12/ekspertyza-04-21-12.pdf>, 05.05.2026.
22. van Deursen, A.J.A.M., Helsper, E.J. (2015). A nuanced understanding of internet use and non-use among the elderly. *European Journal of Communication*, Vol. 30, Iss. 2, pp. 171-187, doi: 10.1177/0267323115578055.
23. van Deursen, A.J.A.M., Helsper, E.J. (2015). The third-level digital divide: Who benefits most from being online? In: M. Graham, W.H. Dutton (Eds.), *Communication and Information Technologies Annual* (pp. 29-52). Bingley: Emerald Group Publishing.
24. van Dijk, J. (2020). *The digital divide*. Cambridge: Polity Press.
25. von Solms, R., van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, Vol. 38, pp. 97-102.

26. Whitman, M.E., Mattord, H.J. (2021). *Principles of information security* (7th ed.). Boston: Cengage.
27. Xie, B. (2025). *Digital literacy impacts quality of life among older adults through technology use and social connectivity*. Scientific Reports.