Grzegorz Strupczewski*

# Mitigating Cyber Risk in Personal Finance of the Elderly. Insights into Vulnerabilities, Cyber Hygiene, and the Role of Personal Cyber Insurance[1]

**Abstract**

The paper investigates the growing cyber threats to personal finance, faced by the elderly in the digital age. It begins by acknowledging the surge in cyber incidents, particularly impacting seniors amid their increasing engagement in the digital space. The research explores the theoretical background of individual attitudes towards cybersecurity, emphasizing the unique vulnerabilities of the elderly population and their heightened susceptibility to cyber threats. It offers practical recommendations for personal cyber hygiene. Moreover, it introduces personal cyber insurance (PCI) and discusses its advantages and challenges. As the main contribution to the body of knowledge, the study provides a comprehensive understanding of the specific challenges faced by the elderly in the digital realm. It offers practical strategies for risk mitigation and introduces PCI as a means of enhancing resilience. It also sets the groundwork for further exploration and targeted strategies to protect individuals, especially older adults, in the dynamic landscape of cybersecurity.

Key words: cybersecurity, cyber risk, cyber threats to the elderly, cyber hygiene, personal cyber insurance

* Assoc. Prof. Grzegorz Strupczewski, PhD, Department of Risk Management and Insurance Cracow University of Economics, e-mail: Grzegorz.Strupczewski@uek.krakow.pl, ORCID: 0000-0002-7882-120X.

1 The article presents the results of Project No. 079/EFZ/2022/POT, which was financed by a subsidy to the Krakow University of Economics.

## Introduction

The 21st-century digital revolution has expanded the potential for mutual communication and data flow, improving economic efficiency and increasing interpersonal dynamics. However, this has resulted in personal dependence on digital technologies and constant internet access, increasing vulnerability to unwanted cyber incidents, such as hacking attacks and leaking confidential data.

In recent years, there has been a significant increase in the number, scale, sophistication, and effectiveness of malicious cyber incidents. This trend has been particularly noticeable since the advent of the COVID-19 pandemic and the prevalence of remote work. The severity of privacy breaches, the rise in cybercriminal activity, and the financial consequences of cyberattacks are all noteworthy. Cyber incidents are a common and expensive cause of interruptions for businesses and public institutions. The digitisation of the economy is increasing, resulting in a denser network of interdependencies in cyberspace. As a result, cyber risk is becoming more systemic. It is important to note that cyber incidents threaten both organisations and individuals. Consumers routinely establish more online accounts, rely on more systemic interconnectivity, and store more personal and sensitive data than at any other time, thus augmenting their personal cyber risk profile[2]. According to the 2023 year-end data released by Statistics Poland, 85,3% of the Polish population used the internet regularly. In the age group of 55–74, this percentage was as high as 63,6%[3].

In recent years, there has been a process of population aging, i.e., an increase in the percentage of elderly people (aged 60 or more) in the country's population. Statistics Poland forecasts that this rate will rise from 25,6% today to 40% in 2050[4]. Rapid development and growth of technology provide a range of novel challenges and opportunities for those currently transitioning into retirement and those who will retire in the future. Technology may provide benefits to retiring adults, offering a solution to difficulties in navigating the

2 R. McGregor, C. Reaiche, S. Boyle, G. Corral De Zubielqui, *Cyberspace and Personal Cyber Insurance: A Systematic Review*, „Journal of Computer Information Systems" 2023, vol. 64, no. 1, p. 157–171.

3 *Digital economy and telecommunications*, https://dbw.stat.gov.pl/dashboard/14 [access: 28.12.2023].

4 A. Bieńkuńska et al., *Jakość życia osób starszych w Polsce*, Warszawa 2020.

transition to retirement. Conversely, technology may lead to additional challenges for those transitioning into retirement, such as an increased vulnerability to online victimisation. All older computer users are potential cyberattack victims and may even unknowingly participate in them. Several studies have identified an increased vulnerability to telemarketing fraud, phishing, pension scams, and other targeted attacks as a manifestation of cyber risk.

In general, cyber risk can be defined as an operational risk associated with the performance of activities in cyberspace, threatening information assets, ICT resources and technological assets, which may cause material damage to tangible and intangible assets of an organisation, business interruption or reputational harm. The term „cyber risk" also includes physical threats to the ICT resources within the organisation[5]. Personal cyber risk diverges from commercial or infrastructure risk insofar that, whilst many cyber threats are comparable across both scenarios (such as malware, phishing, or ransomware), the nature of cyber events, for example, cyber bullying or stalking, at the personal level is often unique to an individual and does not apply to other circumstances. This would suggest that the need of individuals to prevent and protect their „digital selves" within cyberspace, as well as the ability to identify and engage specialist cyber services support, are pivotal to securing a safe online experience, but these capabilities are often not evident or available[6].

To mitigate personal cyber risk, personal accountability and efforts are necessary[7]. However, surveys indicate that consumers simultaneously show significant anxiety about cyber threats, typically putting minimal effort into increasing their cybersecurity and safety[8]. Similarly, the results presented by Zwilling et al.[9] suggest that internet users have sufficient awareness of cyber threats, but they tend to apply only basic and common protective measures.

The purpose of this paper is threefold: (1) to recognize the elderly as an age group particularly exposed to cyberattacks and online fraud and to identify their key vulnerabilities; (2) to provide practical recommendations on protective measures to mitigate personal cyber risk, referred to as

5 G. Strupczewski, *Defining cyber risk*, „Safety Science" 2021, no. 135, p. 6.
6 R. McGregor et al., op. cit.
7 A. Kovacevic, N. Putnik, O. Toskovic, *Factors Related to Cyber Security Behavior*, „IEEE Access" 2020, no. 8, p. 125140–125148.
8 N. Kostyuk, C. Wayne, *The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public*, „Journal of Global Security Studies" 2021, no. 6.
9 M. Zwilling et al., *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*, „Journal of Computer Information Systems" 2022, vol. 62, no. 1, p. 82–97.

personal cyber hygiene; and (3) to present personal cyber insurance as a risk management tool that provides not only cyber loss reimbursement but also assistance after a cyber incident.

The paper is structured as follows. Theoretical background on individual attitudes towards cybersecurity is presented first. The following section outlines vulnerabilities to cyber risks for the elderly as an age group. Practical recommendations on personal cyber hygiene are then provided. These are followed by a section describing and discussing personal cyber insurance. The paper concludes with a final section.

## Theoretical background on an individual attitude to cybersecurity including the Polish perspective

Individual involvement in cyberspace has become a stimulus for academic researchers and practitioners to focus on individual attitudes and behaviours that influence vulnerability to cyber threats[10]. McCormac et al.[11] examined the relationship between information security awareness and individual characteristics like age, gender, personality, and risk-taking propensity. The study revealed that conscientiousness, agreeableness, emotional stability, and risk-taking propensity were significant factors in explaining the variance in individuals' cyber awareness. Additionally, the research has shown a positive correlation between age and cyber awareness. It indicates that older individuals tend to have a better understanding of online security. The study by Zwilling et al.[12] investigated the correlation between cybersecurity awareness, knowledge, and behaviour with protection tools among individuals in general, specifically in Israel, Slovenia, Poland, and Turkey. The results show that higher cyber knowledge is related to the level of cyber awareness, including differences in the respondents' country or gender. L. Hadlington[13] focused on

**10** L.F. Cranor, S. Garfinkel, *Security and usability: Designing secure systems that people can use*, Beijing 2005; B. Schneier, *Secrets and Lies: Digital Security in a Networked World*, Indianapolis 2015.

**11** A. McCormac, *Individual differences and information security awareness*, „Computers in Human Behavior" 2017, no. 69, p. 151–156.

**12** M. Zwilling et al., op. cit.

**13** L. Hadlington, *Employees Attitude Towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom*, „International Journal of Cyber Criminology" 2018, vol. 12, no. 1, p. 269–281.

the relationship between risky employee cybersecurity behaviour, and both individual (such as age and attitude) and organisational factors in protective cybersecurity activities. The study demonstrated that age is a significant factor in determining the frequency of engaging in risky cybersecurity behaviour and attitudes towards cybersecurity. Cain et al.[14] tested the levels of so-called cyber hygiene, which refers to an individual's adherence to best practices for security and protection of personal information. They found that older users engaged in more secure cyber behaviours than younger ones.

The survey report titled „Attitudes of Poles towards cybersecurity" reveals that 85% of the 1084 respondents feel safe using electronic banking despite the occurrence of cyberattacks[15]. Additionally, 52% of Poles report having an antivirus installed and up-to-date smartphone software, with no significant differences across individual age groups. The survey results indicate that a significant number of Poles are willing to incur regular additional expenses to enhance the cybersecurity of electronic banking. This demonstrates a shared responsibility among Poles for building a secure ecosystem of digital services. Specifically, almost 60% of the respondents are willing to accept monthly costs of a few or a dozen PLN. The survey results indicate that 24% of the respondents believe bank customers are responsible for the security of financial electronic services. Most respondents (73%) identified banks as the primary entities responsible for cybersecurity, followed by mobile operators, internet providers, electronic payment operators, and ICT equipment and software vendors. Banks have been leading the way among cybersecurity entities for years, followed by technology companies, the military, the police, and public administration. The respondents placed little trust in social media and online stores. This is despite their immense popularity and impact on daily life.

It is evident that modern technology is not unfamiliar to people aged 60 or more and is increasingly appreciated by them in their daily lives. According to a report by the Polish Bank Association, titled „The Silver Economy"[16], older adults are increasingly active in the digital space. As many as 59% of those

**14** A.A. Cain, M.E. Edwards, J.D. Still, *An exploratory study of cyber hygiene behaviors and knowledge*, „Journal of Information Security and Applications" 2018, no. 42, p. 36–45.

**15** *Badanie „Postawy Polaków wobec cyberbezpieczeństwa"*, ed. 4, https://www.wib.org.pl/wp-content/uploads/2023/07/raport-cyberbezpieczenstwo-2023-postawy-polakow-wobec-cyberbezpieczenstwa.pdf [access: 21.12.2023].

**16** *Srebrna gospodarka*, Warszawa 2022, https://bank.pl/wp-content/uploads/2022/10/Raport_Srebrna-gospodarka.pdf [access: 21.12.2023].

surveyed reported no issues contacting their bank, and 80% of the seniors who use the internet manage their finances through mobile or online banking. As many as 88% of the seniors report having a payment card, with 70% using it frequently. The population of elderly people aged 60 or more differs significantly from typical bank customers, possessing more free time, better financial assets, and a steady retirement income. Additionally, seniors have formed interests, and require more attentive and understanding communication, due to diminished perceptual and cognitive abilities and a greater need for daily support and healthcare[17]. It is important to note that approximately 40% of individuals aged 65–69 are economically active. Moreover, around 20% of individuals aged 70–74 continue to work. However, the percentage of seniors working at the age 75 or more significantly decreases.

## Seniors as an age group with particularly high vulnerability to cyber risk

Although elderly people rarely report being victims of financial cybercrime, evidence suggests that older Internet users are at an increased risk. This is due to factors such as social isolation, cognitive, physical, and mental problems, wealth status, limited cybersecurity skills or awareness, social attitudes, and the content of online scams[18].

The FBI's „Elder Fraud Report" revealed that 88262 individuals aged 60 or more fell victims to financial fraud carried out via the Internet in 2022, marking a 47% increase in relation to 2018[19]. This age group accounted for 21,6% of all online fraud victims. Seniors suffered an average loss of $ 35101. This is significantly higher than in other age groups. The report also identifies the most common types of online fraud that seniors aged 60 or more fall prey to. The following are the top ten types of online fraud: (1) false technical support leading the victims to disadvantage their funds, (2) non-delivery of goods purchased online, (3) theft of personal information, (4) matrimonial fraud,

**17** Ibidem, p. 7.

**18** A. Burton et al., *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review*, „Experimental Gerontology" 2022, vol. 159, no. 111678.

**19** *Elder Fraud Report*, Federal Bureau of Investigation, 2022, p. 4, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf [access: 22.12.2023].

(5) theft of credit card details, (6) identity theft, (7) false investment, (8) blackmail to extort ransom, (9) impersonation of a known institution, and (10) phishing[20]. However, fraudulent investments are the most financially damaging.

Burton et al.[21] provide a comprehensive explanation of why, how and in what contexts older people can become victims of online financial crime (aka scams).

1. If the content of a scam includes a threat, a request for help, or a promise of a reward, it can provoke an emotional response from the user. This emotional response can increase the likelihood that the user will respond positively to the criminal's request. It is important to remain objective and avoid emotional language when discussing scams. Fraudulent emails often contain persuasive techniques designed to elicit emotional, spontaneous responses by appealing to the sympathy for others, and the need for financial and emotional security, such as threats of negative consequences. Phishing emails increase anxiety associated with not responding, for example, by stating, „If you do not contact us by the following date, your account may be closed". Befriending or persuasion techniques, such as identifying with the victim's qualities, have been found to be particularly effective with older people who are socially isolated. Emotional comments can encourage impulsive decision-making, increasing the likelihood of falling for a scam, especially when it requires a quick response, as in the case of emails titled „Urgent help needed".

2. Older individuals are more susceptible to responding to scams from seemingly legitimate sources, such as reputable companies or government agencies, due to their greater trust in authority. Scammers often impersonate organisations, including banks, police, or government agencies, to deceive people into providing personal or financial information. This is often done by claiming payment issues, account security, or overdue refunds.

3. If elderly individuals lack digital skills or cybersecurity awareness, they may perceive the risk of cyberattacks as low and may not be motivated to seek information on protecting themselves from cyber threats. This increases the likelihood of falling victim to cybercriminals. Older individuals may have limited digital skills or cybersecurity awareness due to less exposure to technology. Research has shown that those who have previously used computers at work

**20** Ibidem, p. 6.
**21** A. Burton et al., op. cit.

tend to have better cybersecurity skills and are more motivated to learn new skills. Limited technical competence has been associated with decreased awareness of digital vulnerability. This can result in less motivation to seek protection and a reduced ability to search for cybersecurity information and identify fraud attempts.

4. If the elderly have limited awareness of cyber threats, they may perceive the risk of becoming a victim of a cyberattack as low. This perception, combined with high online activity, may increase the possibility of being targeted by criminals. Careless use of technology, increased online visibility, and uncontrolled sharing of personal information can result from low risk perception or a lack of understanding of security risks. Criminals frequently target social networks, where novice users are more likely to disclose their personal information due to a lack of awareness of the dangers of disclosure. Additionally, novice users are more likely to leave Wi-Fi and Bluetooth permanently on, putting their data at risk of theft. A study revealed that older individuals are aware of phishing, but they lack awareness of their own vulnerability and how their behaviour can put them at risk.

5. If older individuals lack cybersecurity skills, they may also be less familiar with the language and terminology used in digital security. This can make it more difficult for them to identify suspicious individuals or emails, ultimately increasing their risk of being targeted in cyberattacks. However, it is not fully confirmed. According to a 2021 study, older individuals were more adept at detecting fraudulent emails and exhibited greater vigilance in identifying them.

6. If older individuals are more inclined to seek quick and simple solutions for accessing online services, they may be more likely to use unsecured Wi-Fi networks, seek advice from individuals with limited expertise, and are less likely to use PIN codes or biometric security. This increases the opportunities for criminals to attack them.

7. If an older adult experiences a decline in health and mobility, they may increasingly rely on online banking, online shopping, remote healthcare, and social media. This increased reliance may lead to more frequent sharing of personal information, resulting in greater online visibility and an increased risk of cyberattacks.

8. If an older adult experiences memory issues, they may struggle to recall the details of an online scam or even be unaware that they were scammed. This can lead to a failure to report the incident to a law enforcement agency, which increases the risk of being scammed again.

9. If seniors experience cognitive deficits such as impaired judgment, impulsivity, or reduced perceptual speed, they may have difficulty understanding and evaluating the consequences of their choices, particularly under time pressure. This can increase their risk of becoming a victim. Cognitive function deterioration can impede the user's ability to comprehend and evaluate choices, particularly under time pressure. This may be linked to challenges with tasks that necessitate divided attention or reduced processing speed. Changes in the cerebral cortex have been linked to heightened gullibility and susceptibility to suggestion in individuals with cognitive impairments, as well as age-related changes in risky decision-making. These deficits may decrease the likelihood of following recommended safety measures. A minor interruption caused by a pop-up can increase a senior's vulnerability to scams due to the increased cognitive load that requires divided attention.

10. If a senior is grieving for a partner who was responsible for financial affairs, taking on new and unfamiliar financial responsibilities during a time of stress and grief can impair their ability to identify fraud and increase their risk of becoming a victim.

11. Socially isolated seniors are at an increased risk of falling victim to fraud due to limited opportunities to discuss potential scams and seek advice from others.

12. If an older adult is experiencing loneliness, scammers may use social influence tactics, such as identifying with the victim's traits or using befriending or grooming techniques, to increase the likelihood of the older adult falling prey to the scam or criminal activity.

13. If an older adult is single, their online visibility and trust in strangers may increase as they seek contact with others online, leading to an increased risk of financial cybercrime.

14. Elderly individuals with a diverse range of high-value assets may be more susceptible to financial attacks and less likely to detect and report such crimes, making them vulnerable to repeat victimisation.

15. When financial cybercrime is not perceived as a serious issue by society, and prevailing attitudes condemn the victim, older people may experience embarrassment, shame, and fear of not being taken seriously. This can make them less likely to disclose being a victim, which increases the risk of being scammed again.

16. When seniors are considered vulnerable by society, they may be less likely to report being a victim of a crime. This can increase the risk of repeat violence as they may fear losing their independence or being restricted.

## Cyber hygiene recommendations

Individuals can reduce cyber risk by practicing personal cyber hygiene. This refers to the habits and practices adopted to maintain a secure digital environment. It involves taking proactive measures to safeguard personal information, devices, and online activities from potential cyber threats. Personal cyber hygiene practices are as follows:

1. Use Strong and Unique Passwords: Individuals should create complex passwords for each online account. Combining uppercase and lowercase letters, numbers, and special characters enhances password strength.

2. Implement Two-Factor Authentication (2FA): Enable 2FA whenever possible to add an extra layer of security to online accounts. This involves providing a secondary form of authentication, such as a code sent to a mobile device.

3. Regularly Update Software: Keep the operating systems, applications, and security software up to date to patch vulnerabilities. Regular updates are crucial for maintaining a secure digital environment.

4. Be Cautious of Phishing Attempts: Exercise caution when clicking on links or providing personal information online. Verify the legitimacy of emails and avoid interacting with suspicious messages.

5. Perform Regular Data Backups: Back up important files regularly to mitigate the impact of data loss. Storing backups in multiple locations, such as external drives or secure cloud services, is recommended.

6. Configure Privacy Settings: Adjust privacy settings on social media platforms and online services to control the amount of personal information shared. Regularly review and update these settings.

7. Secure Wi-Fi Networks: Use strong passwords and encryption protocols for home Wi-Fi networks. Avoid sensitive activities on public Wi-Fi and consider using VPNs for added security.

8. Implement Device Security Measures: Enable device encryption to protect data in case of theft. Set up screen locks on devices and install reputable security software.

9. Stay Informed about Cybersecurity Threats: Regularly educate yourself on the latest cybersecurity threats and trends. Awareness is a key element in preventing falling victim to evolving cyber threats.

10. Practice Safe Online Shopping: When shopping online, use secure and reputable websites, and avoid saving payment information on multiple sites. This reduces the risk of financial information exposure[22].

However, even the most cautious and tech-savvy individuals can never be completely risk-free. This is where personal cyber insurance comes in handy, as it can help reduce the risk and transfer the potential for loss from that residual risk. Although not yet widely available, personal cyber insurance is expected to become a fast-growing market segment due to the rapidly increasing exposures consumers face today[23].

The survey titled „Attitudes of Poles towards Cybersecurity" reveals that a significant share of Poles are aware of the most critical principles of cyber hygiene in the context of digital finance[24]. The respondents declared adherence to bank recommendations such as:

– not giving passwords and payment card details to strangers (78%),
– not opening suspicious attachments and links from unknown senders (74%),
– not storing banking login information on a smartphone (65%),
– carefully reading text messages and notifications from online banking (63%),
– not giving out important personal information on social media (54%),
– setting transaction limits in online banking (52%).

When analyzing the attitudes of seniors, it is essential to note that individuals aged 65 or more adhere to the recommended behaviours outlined above. In fact, seniors are leaders in password and payment card security, as well as in exercising caution in opening attachments and links, compared to other age groups.

## Personal cyber insurance

During the late 1990s, general insurers introduced cyber insurance as a distinct product segment to offer commercial customers a traditional risk transfer

**22** S. Baraković, J. Baraković Husić, *Cyber hygiene knowledge, awareness, and behavioral practices of university students*, „Information Security Journal: A Global Perspective" 2023, vol. 32, no. 5, p. 347–370; A.A. Cain et al., op. cit.

**23** *Personal cyber insurance: Protecting our digital lives*, Swiss Re 2019, https://www.swissre.com/dam/jcr:68e4d8fb-509c-4182-a219-c803f7d23af1/ZRH-18-00632-P1_Personal_cyber_insurance_Publication_WEB.pdf [access: 23.12.2023].

**24** *Badanie „Postawy Polaków…*

option for the emerging and ubiquitous digital peril[25]. The introduction of personal cyber insurance (PCI) is a recent development that has emerged due to the public realising that individuals are more vulnerable to cyber incidents than organisations. This is because individuals typically have fewer resources and less expertise to enhance their cyber defence capabilities. Additionally, they are often inadvertent victims of third-party data breaches[26].

Personal cyber insurance is not yet a mass-market product like typical motor, property, or health insurance. Currently, most PCI policies only cover first-party loss, i.e., damage to one's property following a cyber incident. Few products provide coverage for third-party liability claims resulting from the insured person's acts or omissions in the digital world. This text fragment appears to meet the desired characteristics. No changes were made.

## Scope of insurance coverage

Personal cyber insurance provides a strong defence against the complex challenges which individuals face in today's digital age. It offers coverage beyond financial compensation, addressing concerns related to privacy, security, and personal well-being.

An important aspect of this coverage is protection against identity theft, being a common cyber threat. Personal cyber insurance can help mitigate the consequences of identity-related crimes, such as the unauthorised exploitation of personal information for fraudulent activities. This type of insurance covers the misuse of sensitive data, including social security numbers and financial account details. Additionally, it provides coverage against unauthorised access to personal accounts, which further fortifies financial security. This aspect ensures that individuals are protected from the financial consequences of cybercriminals gaining unauthorised access to their banking, investment, or other monetary platforms. Unauthorised access can lead to illicit transactions, and PCI serves as a critical deterrent against resulting financial losses.

In the digital realm, financial fraud is a constant threat. Cyber insurance provides coverage for losses resulting from financial fraud, protecting against the financial consequences of fraudulent transactions initiated by cyber

**25** R. McGregor et al., op. cit.
**26** A.A. Cain et al., op. cit.

criminals. This includes unauthorised transfers, credit card fraud, and other monetary losses incurred due to cyber-enabled financial crimes. In addition, PCI provides financial protection for costs related to data breaches, such as expenses for forensic investigations, notification procedures, and credit monitoring services for affected individuals. The coverage addresses tangible financial losses as well as recognizes the intangible costs associated with compromised data.

Cyber extortion falls under the insurance umbrella, covering threats and demands for ransom in exchange for releasing compromised digital assets. Personal cyber insurance offers financial protection, covering the costs associated with cyber extortion incidents and facilitating the recovery process. Table 1 provides detailed characteristics of PCI coverage, along with sample loss scenarios.

Table 1. Insurance coverage for cyber risks for individuals with sample loss scenarios

| Scope of insurance coverage | Description of insurance coverage | Sample damage scenarios |
|---|---|---|
| Financial fraud | – Coverage of financial losses resulting from unauthorised use of electronic payment services<br>– Coverage of the cost of blocking and reissuing a payment card | The victim of a phishing attack revealed his e-banking login information, resulting in the theft of funds from his bank account |
| Online shopping | –Reimbursement for the cost of goods purchased online that were not delivered, damaged during delivery or delivered in error | The victim purchased from a fake online store and, as a result, lost the money paid for goods that were never delivered |
| Identity theft | – Reimbursement of the cost of reserving and making new documents, making appropriate notations in public records and concluding contracts<br>– Consultation with a consultant on the recovery or restoration of data relevant to digital identity or financial records | As a result of the theft of personal information from an online store, the victim's credit card data was leaked and sold on the darknet. They were then used to make unauthorised purchases. There is an urgent need to restrict the card and protect against the consequences of identity theft |
| Data recovery | – Paying for the cost of an IT specialist to remove malware from hardware and to restore corrupted data | An infected flash drive transfers malware to a computer, leading to data loss or corruption. The services of an IT specialist are needed to isolate and remove the malware and then to restore the data from a backup |

| Scope of insurance coverage | Description of insurance coverage | Sample damage scenarios |
|---|---|---|
| Cyber bullying | – Covering the costs of reducing and mitigating the effects of unlawful harassment or defamation of the victim through social media, such as consultation with a psychologist, legal advice, relocation, and protection of online reputation (by removing or hiding private content)<br>– Liability of parents for claims brought against them in connection with cyber bullying committed by their children | – The child becomes a victim of a cyber bullying campaign on social media, putting the family under stress. The child needs professional help from a psychologist to better cope with the situation. In addition, a change of school is necessary<br>– A child harasses a schoolmate on social media. There is a risk of a lawsuit due to an alleged failure of parental supervision |
| Cyber extortion | – Reimbursement of the cost of the ransom paid.<br>– Providing an IT specialist to limit the negative effects of cyber extortion | By clicking on a malicious link on a website, the victim inadvertently infects their computer with ransomware that encrypts all data. This is followed by a ransom demand to send the key that unlocks the data. |
| Liability for cyber incidents | – Liability for claims brought against the insured in connection with the exchange or transfer of digital data or the use of the insured person's information systems.<br>– Liability for claims brought against the insured person for the infringement of third-party personal rights or copyright. | – One of the victim's smart home devices was infected with malware and used as part of a cyberattack carried out without the victim's knowledge<br>– The insured person posted the company's copyrighted logo on his personal blog without obtaining proper permission |

Source: *Personal cyber insurance...*, p. 11.

## Key exclusions from insurance coverage

While PCI offers a comprehensive safeguard against an array of cyber risks, it is imperative to acknowledge the nuances of its limitations through a thorough examination of exclusions. Understanding these exclusions is crucial for individuals to appreciate the scope and boundaries of their coverage, ensuring informed decision-making.

One fundamental exclusion involves deliberate and fraudulent actions by the policyholder. Personal cyber insurance typically does not cover losses incurred because of intentional and fraudulent activities undertaken by the

insured individual. This exclusion is in place to discourage malicious behaviour and to maintain the integrity of the insurance contract.

Exclusions may extend to losses incurred due to inadequate cybersecurity measures. If an insured individual fails to adhere to industry-standard cybersecurity practices, such as regularly updating software or employing robust password protection, and a cyber incident occurs, the resultant losses may not be covered. This emphasizes the importance of proactive cybersecurity measures in maintaining the insurability of digital assets.

Another exclusionary consideration involves losses incurred due to the failure to comply with security protocols specified in the insurance policy. If an insured individual neglects to follow prescribed security procedures, such as reporting incidents promptly or cooperating in the investigation process, it may lead to the exclusion of certain claims.

In summary, the exclusions in personal cyber insurance serve to delineate the boundaries of coverage and also to incentivise responsible cybersecurity practices among policyholders. By understanding and adhering to these exclusions, individuals can optimise the effectiveness of their cyber insurance coverage.

## Advantages and disadvantages of PCI

Personal cyber insurance offers valuable protection against an array of cyber risks. However, individuals must carefully weigh the pros and cons, considering cost factors, policy complexity, and the need for ongoing cybersecurity diligence to make informed decisions about coverage. The major advantages of PCI are as follows:

1. Financial protection against cyber threats: PCI serves as a financial safety net, offering coverage for a range of cyber threats, including identity theft, financial fraud, and data breaches.
2. Legal support: In the event of a cyber-related lawsuit, PCI may provide coverage for legal expenses, offering individuals the required support to navigate the complex legal landscape associated with cyber incidents.
3. Comprehensive coverage: The scope of PCI is extensive, covering not only direct financial losses but also expenses related to forensic investigations, notification procedures, and credit monitoring services after a data breach.
4. Risk mitigation: By providing coverage for cyber threats, PCI encourages individuals to adopt proactive cybersecurity measures, fostering a culture of risk awareness and mitigation.

5. Customisation: Policies can be tailored to the specific needs and risk profiles of individuals. This allows for a personalised approach to cybersecurity coverage based on the nature of digital activities and assets.

Certain disadvantages of PCI can also be pointed out, which include:

1. Exclusions and limitations: PCI policies often come with exclusions and limitations, such as intentional fraudulent actions by the policyholder, pre-existing vulnerabilities, and losses due to inadequate cybersecurity measures. Understanding these limitations is crucial for effective coverage.

2. Cost: The premiums for PCI can be relatively high, and the cost-effectiveness of the coverage may vary depending on the individual's risk profile and the level of protection needed.

3. Complexity of policies: The language and terms in PCI policies can be complex and may require a deep understanding of cybersecurity concepts. Individuals may find it challenging to grasp the intricacies of the coverage they are purchasing.

4. Dependency on individual cyber hygiene: The effectiveness of PCI is contingent on the insured person's adherence to cybersecurity best practices. Neglecting these practices may lead to exclusions and limitations in coverage.

5. Evolution of cyber threats: As cyber threats are continually evolving, personal cyber insurance policies may need regular updates to ensure that they remain effective against the emerging risks. Staying abreast of the changing cybersecurity landscape is essential for maintaining comprehensive coverage.

## Conclusions

As society becomes more reliant on technology, the importance of cyber threats and cyber insurance is growing. Private consumers acknowledge the need for a solution to counteract threats originating from cyberspace. The paper explores the increased cyber risks that the elderly face in an increasingly digital era. It combines theoretical insights into individual cybersecurity attitudes, emphasizing the unique vulnerabilities of older individuals. The study reveals that, contrary to common perceptions, seniors often exhibit better cyber hygiene than their younger counterparts. Seniors are susceptible to cyber threats due to social isolation, cognitive limitations, and limited cybersecurity skills. The paper proposes practical recommendations for personal cyber hygiene to underscore the importance of proactive measures. Additionally,

the paper introduces personal cyber insurance as a vital risk management tool. Insurance can play a crucial role in safeguarding customers against cyber threats. Cyber insurance can provide individuals with many benefits, including support in enhancing cybersecurity, financial compensation, and expert assistance following a cyber incident. However, insurance companies must develop products that cater to the needs of a new generation of digitally connected consumers to maximise their growth opportunities.

To recapitulate, this paper provides a thorough analysis of the risks and vulnerabilities that elderly individuals face in the digital world, along with practical strategies to mitigate those risks. The research serves as a basis for further exploration and for developing targeted strategies to protect individuals, particularly the elderly, in the constantly evolving digital landscape.

## Bibliography

*Badanie „Postawy Polaków wobec cyberbezpieczeństwa"*, ed. 4, https://www.wib.org.pl/wp-content/uploads/2023/07/raport-cyberbezpieczenstwo-2023-postawy-polakow-wobec-cyberbezpieczenstwa.pdf [access: 21.12.2023].

Baraković S., Baraković Husić J., *Cyber hygiene knowledge, awareness, and behavioral practices of university students*, „Information Security Journal: A Global Perspective" 2023, vol. 32, no. 5.

Bieńkuńska A., Ciecieląg P., Góralczyk A., Haponiuk M., *Jakość życia osób starszych w Polsce*, Warszawa 2020.

Burton A. Cooper C., Dar A., Mathews L., Tripathi K., *Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review*, „Experimental Gerontology" 2022, vol. 159, no. 111678.

Cain A.A., Edwards M.E., Still J.D., *An exploratory study of cyber hygiene behaviors and knowledge*, „Journal of Information Security and Applications" 2018, no. 42.

Cranor L.F., Garfinkel S., *Security and usability: Designing secure systems that people can use*, O'Reilly, Beijing 2005.

*Digital economy and telecommunications*, https://dbw.stat.gov.pl/dashboard/14 [access: 28.12.2023].

*Elder Fraud Report*, Federal Bureau of Investigation, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf [access: 22.12.2023].

Hadlington L., *Employees Attitude Towards Cyber Security and Risky Online Behaviours: An Empirical Assessment In The United Kingdom*, „International Journal of Cyber Criminology" 2018, vol. 12, no. 1.

Kostyuk N., Wayne C., *The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public*, „Journal of Global Security Studies" 2021, no. 6.

Kovacevic A., Putnik N., Toskovic O., *Factors Related to Cyber Security Behavior*, „IEEE Access" 2020, no. 8.

McCormac A., Zwaans T., Parsons K., Calic D., Butavicius M., Pattinson M., *Individual differences and information security awareness*, „Computers in Human Behavior" 2017, no. 69.

McGregor R., Reaiche C., Boyle S., Corral De Zubielqui G., *Cyberspace and Personal Cyber Insurance: A Systematic Review*, „Journal of Computer Information Systems" 2023, vol. 64, no. 1.

*Personal cyber insurance: Protecting our digital lives*, Swiss Re 2019, https://www.swissre.com/dam/jcr:68e4d8fb-509c-4182-a219-c803f7d23af1/ZRH-18-00632-P1_Personal_cyber_insurance_Publication_WEB.pdf [access: 23.12.2023].
Schneier B., *Secrets and Lies: Digital Security in a Networked World*, Indianapolis 2015.
*Srebrna gospodarka*, Warszawa 2022, https://bank.pl/wp-content/uploads/2022/10/Raport_Srebrna-gospodarka.pdf [access: 21.12.2023].
Strupczewski G., *Defining cyber risk*, „Safety Science" 2021, no. 135.
Zwilling M., Klien G., Lesjak D., Wiechetek Ł., Cetin F., Basim H.N., *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*, „Journal of Computer Information Systems" 2022, vol. 62, no. 1.

# Ograniczanie ryzyka cybernetycznego w finansach osobistych osób starszych. Podatności na cyberzagrożenia, cyberhigiena i rola prywatnego ubezpieczenia cybernetycznego

**Streszczenie**

Artykuł dotyczy cyberzagrożenia finansów osób starszych w erze cyfrowej. Wzrost liczby incydentów cybernetycznych szczególnie dotyka osoby starsze w związku z ich rosnącym zaangażowaniem w przestrzeń cyfrową. Autor wskazał teoriopoznawcze podstawy indywidualnych postaw wobec cyberzagrożeń, podkreślił przesłanki wyjątkowo dużej wrażliwości osób starszych. Następnie zaproponował praktyczne zalecenia dotyczące osobistej cyberhigieny w codziennych interakcjach z usługami cyfrowymi. Ponadto przedstawił istotę ubezpieczenia ryzyk cybernetycznych dla osób prywatnych, ocenił jego zalety i wady. Autor artykułu dokonał kompleksowej analizy specyficznych wyzwań stojących przed osobami starszymi w sferze cyfrowej, zaproponował praktyczne strategie ograniczania ryzyka wraz z prywatnym ubezpieczeniem cybernetycznym jako narzędziem zwiększania odporności cyfrowej i ograniczania szkód. Artykuł stanowi podstawę do dalszych badań i formułowania strategii ochrony osób, zwłaszcza starszych, w dynamicznym świecie finansów cyfrowych.

Słowa kluczowe: cyberbezpieczeństwo, ryzyko cybernetyczne, cyberzagrożenia wobec osób starszych, cyberhigiena, prywatne ubezpieczenie cybernetyczne