

Knowledge and Awareness of Digital Threats: Asymmetry Between Perceived Vulnerability and Severity Among Generation Z

Tomasz Eisenhardt¹, Monika Eisenhardt² and Alicja Fandrejewska-Nowakowska³

¹University of Warsaw, Poland

²University of Economics in Katowice, Poland

³Warsaw University of Life Sciences, Poland

teisenhardt@wz.uw.edu.pl

monika.eisenhardt@ue.katowice.pl

alicja_fandrejewska@sggw.edu.pl

Abstract: The rapid expansion of digital technologies has increased users' exposure to cybersecurity threats, making knowledge and awareness critical components of safe participation in digital environments. This study aims to assess the level of knowledge and awareness of digital threats among Generation Z, with a particular focus on the asymmetry between perceived vulnerability and perceived severity. The research is based on a quantitative survey conducted using the CAWI method among 770 respondents. The analysis includes both descriptive statistics and non-parametric tests (Mann–Whitney U and Kruskal–Wallis) to examine differences across socio-demographic characteristics. The results indicate a clear asymmetry in risk perception: while respondents assess their vulnerability to cyber threats as moderate, they simultaneously perceive the potential consequences as highly severe. Additionally, perceived vulnerability varies significantly across selected socio-demographic variables, whereas perceived severity remains relatively uniform. These findings suggest that Generation Z demonstrates a differentiated structure of cybersecurity awareness, characterized by a stronger internalization of risk consequences than personal exposure. The study contributes to the literature by providing empirical evidence on the relationship between perceived vulnerability and severity in the context of digital threats. The findings have practical implications for the design of educational and awareness-raising initiatives, highlighting the need to strengthen users' perception of their own exposure to cyber risks.

Keywords: Cybersecurity awareness, Digital threats, Perceived vulnerability, Perceived severity, Generation Z, Cyber risk perception, Digital competences

1. Introduction and the Research gap

The rapid expansion of digital technologies and increased reliance on online services have fundamentally transformed contemporary societies and economies. Growing reliance on digital platforms for communication, education, finance, and public services increases efficiency, accessibility as well as exposure to threats such as cybercrime, phishing, and identity theft. As a result, cybersecurity has become a critical aspect of everyday user behaviour and decision-making. Knowledge and awareness of digital threats are key to ensuring safe participation in the digital environment. Effective cybersecurity depends on technological solutions and regulatory frameworks as well as individuals' ability to recognize risks, assess their potential consequences, and respond appropriately. Previous research highlights that human factors, including limited awareness, cognitive biases, and insufficient digital competences, often constitute the weakest link in cybersecurity systems. Also, risk perception is not uniform and may vary depending on individual characteristics and experiences.

Generation Z, also known as digital natives, is a particularly important group in this regard. Previous studies indicate that their intensive use of digital technologies does not always align with levels of knowledge and awareness (Fandrejewska et al., 2025). Despite high engagement with digital technologies and online services, their awareness of cybersecurity risks remains ambiguous. Frequent use of digital tools does not necessarily translate into accurate risk assessment or responsible behaviour. Moreover, users are increasingly targeted by sophisticated cyberattacks that exploit psychological mechanisms, such as social engineering and manipulation.

Despite a well-developed literature on cybersecurity and digital competences, empirical research on users' perceptions of cyber risk dimensions remains limited, particularly regarding the relationship between perceived vulnerability and perceived threat severity. Understanding this relationship is essential, as discrepancies between these dimensions may influence users' behaviour and risk-taking.

The study addresses this research gap by examining the level of knowledge and awareness of digital threats among Generation Z, focusing on the asymmetry between perceived vulnerability and perceived severity. By analysing how young users assess their exposure to cyber threats and their potential consequences, the study provides empirical evidence on the structure of cybersecurity awareness. The findings enhance our

understanding of the human side of cybersecurity and have implications for the design of educational programs and policies to improve digital safety.

2. A Literature Review

2.1 Digital e-Services and Cybersecurity Challenges

Digital e-services are widely regarded as a response to societal challenges such as workforce shortages, population aging, and limited resources. Bridging digital divides is critical for sustainable digitalized societies (Vassilakopoulou & Hustad, 2021), as high-speed Internet underpins daily life, economic participation, and interaction with government (Sanders & Scanlon, 2021). Digital inclusion also raises broader questions about how policies, organizations, and technologies can converge within national environments, contributing to the development of digital nations (Al-Muwil et al., 2019). However, social needs cannot be met, and e-services cannot reach users adequately unless they are reliable, stable, accessible, and secure.

One of the key aspects in this context is consumer safety and cybersecurity. Authorities strive to increase security and protect consumers from cyberspace risks. However, the pace of change makes it very difficult to keep up with technological advancements. The existing legal framework remains insufficient, and although self-regulation, ethical approaches, and transparency are increasingly emphasized, they are not adequate on their own. Cyberattacks on enterprises fall into three categories: malware, identity theft, and service disruption, with consequences ranging from financial and reputational losses and operational interruptions to societal disruptions and legal repercussions, including violations of EU data protection regulations (Nowak, 2020; Greser, 2021, p. 106).

In the contemporary digital economy, the radical shift toward remote transactions and e-services has made cyberattacks a major disruptor to their development. Modern digital ecosystems face many cybersecurity threats that exploit vulnerabilities in legacy equipment and systems, as well as technical flaws and human weaknesses, negligence, or errors. Malicious software, such as viruses, ransomware, and botnets, can steal sensitive data or disable critical infrastructure, often resulting in legal and financial liability and reputational damage. Despite warnings and proactive prevention efforts, the number of cyberattacks continues to grow, and the forms and technological solutions used in these attacks are constantly evolving (CERT Polska, 2025, 2026).

The COVID-19 pandemic accelerated the shift of business processes to online environments, increasing vulnerability to cyberattacks when traditional access controls were replaced by new tools (Government of Poland, n.d.). Also, as Schabikowska (2025) points out, “cybercriminals continually improve their methods”. In 2024, the CERT Polska team recorded 103,449 security incidents, with reported cases rising 62% and incidents rising 29% compared to 2023 (CERT Polska, 2025; NASK, 2024). The average cost of downtime resulting from an incident reached PLN 1.3 million, though total costs, including data loss and reputational harm, are difficult to estimate (Government of Poland, n.d.). Notably, only 3% of Polish companies have achieved a mature level of cybersecurity readiness (Cisco, 2025).

Apart from technical infections, attackers use social engineering (Heartfield & Loukas, 2015) and AI-driven tactics (Basit et al., 2021). For instance, phishing (Lastdrager, 2014) may exploit human behavior to compromise organizational and personal security, which stresses that human vulnerability may be seen as a significant weakness in a defensive framework. Insider threats, involving malicious actors, rival entities, former employees, or negligent personnel, constitute an additional significant source of cyber risk (Alzaabi et al., 2024; Urbanek, 2024). Protecting e-services requires technical measures combined with an organizational culture ensuring continuous security awareness.

Malware is growing at an alarmingly high rate, making early identification critical (Aslan & Samet, 2019), and ransomware has highlighted the dangers of malicious software, affecting private users, corporations, public services, governments, and security institutions (Or-Meir et al., 2019). Beyond a technical issue, malware serves as a tool for breaching security and seizing control of devices. It is distributed via malicious messages, fake links, and applications posing as legitimate programs, targeting sensitive data, extorting money, and building botnets for large-scale attacks (Wolny, 2020; CBZP, 2025). Thus, the effectiveness of modern cyberattacks lies not only in exploiting technical vulnerabilities but primarily in manipulating human psychology and emotions.

2.2 Digital Competences as a key Factor of Cybersecurity (DigComp 3.0)

Given the wide range of online threats, from dishonest commercial practices to cybersecurity risks, users need to develop adequate digital knowledge, awareness, and competencies. There are numerous and increasingly sophisticated threats in the online environment, including various forms of malicious software and cyberattacks

(PDP UW, 2026). These risks encompass, among others, malware damaging systems or stealing data, spyware monitoring user activity, ransomware encrypting data and demanding payment in return for its release, and distributed denial-of-service (DDoS) attacks making services unavailable to consumers. In addition, users are exposed to phishing and related social engineering techniques that attempt to deceive individuals into revealing sensitive information or performing harmful actions by impersonating trusted institutions or individuals. Unfortunately, the number of cyberattacks is increasing, and their scale is growing (NASK, 2024; Bochyńska, 2026). While cyberattacks were once assumed to target mainly large organizations, individuals are equally at risk since their personal, financial, and sensitive data are frequently compromised and exploited. It is true that the legal and reputational consequences primarily affect organizations; however, it is individual users who are exposed to various types of risks.

Advanced technologies such as AI, ML, big data analytics, and IoT influence the sophistication and scale of malicious practices. They enable more precise behavioral analysis, more powerful DDoS attacks, and increasingly convincing synthetic media in the form of images, audio and video. Misinformation and disinformation are pervasive, and fake news can easily spread via social media (Mahmoudi et al., 2024; Mahmoudi et al, 2025). Regardless of whether such content is shared intentionally or unintentionally (Lipińska et al., 2025), its impact can be very far-reaching.

The knowledge, awareness, and digital competences of consumers are crucial, as they safeguard users in the digital environment as emphasized in previous research on digital consumer behavior (Fandrejewska-Nowakowska et al., 2026). An adequate level of these competences enables internet users to search for information effectively, critically evaluate it, and use it in an informed and secure manner when accessing e-services. It is essential to systematize existing knowledge and to organize the process of assessing and developing digital competences effectively. One widely used reference is the European Digital Competence Framework 3.0 (Cosgrove & Cachia, 2025), which defines digital competence and supports its development across different proficiency levels.

The DigComp 3.0 distinguishes five key areas of digital competence. The first is information and data literacy, which involves the ability to search for, filter, critically assess, and manage information and data originating from various digital sources. The second area, communication and collaboration, concerns effective and responsible communication and cooperation in digital environments, including sharing content, adhering to netiquette, managing digital identity, and participating in online communities. The third, digital content creation, covers the creation and editing of digital content, the integration of different formats, a basic understanding of programming, as well as respect for copyright and licensing rules. The fourth area, safety, wellbeing and responsible use, relates to the protection of devices, personal data and privacy, coping with cybersecurity threats, safeguarding mental and physical wellbeing online, and understanding digital rights and responsibilities. Finally, problem-solving refers to the use of digital technologies to solve problems, identify needs, select appropriate tools, experiment creatively, and continuously update one's competences in line with technological developments, including those linked to artificial intelligence.

3. Research Methodology

3.1 Research Questions and Hypotheses

The main objective of this study is to assess the level of knowledge and awareness of digital threats among Generation Z, with particular emphasis on perceived vulnerability to cybercrime and the assessment of the potential harm associated with such threats.

Based on this objective, the following research questions are formulated:

RQ1: *Are there differences in the perception of vulnerability and potential harm among respondents?*

RQ2: *How do Generation Z respondents assess their vulnerability to cybercrime and personal data interception?*

To address RQ2, a set of hypotheses was formulated assuming that perceived vulnerability to cybercrime varies across selected socio-demographic variables, including gender (**H2a**), level of education (**H2b**), professional status (**H2c**), place of residence (**H2d**), and financial situation (**H2e**).

RQ3: *How do Generation Z respondents evaluate the potential harm associated with digital threats?*

Similarly, for RQ3, it is assumed that perceived severity of cybercrime differs across the same socio-demographic variables, namely gender (**H3a**), level of education (**H3b**), professional status (**H3c**), place of residence (**H3d**), and financial situation (**H3e**).

To address these research questions, two main analytical directions were adopted (Table 1):

Table 1: Variables used for analytical purposes

Analytical direction	Variable	Description and conceptual meaning	Related research questions
Assessment of perceived vulnerability to digital threats	General vulnerability to cybercrime (CP1)	Self-assessed vulnerability to cybercrime, including hacking, phishing, fraud, and malware	RQ2
	Vulnerability to personal data interception (CP3)	Self-assessed vulnerability to unauthorized access to personal data	RQ2
Assessment of perceived severity (potential harm) of digital threats	Perceived harm of cybercrime (CP2)	Perceived seriousness of the potential consequences of cybercrime	RQ3
	Perceived harm of personal data interception (CP4)	Perceived seriousness of the potential consequences of personal data theft or interception	RQ3

3.2 Research Design and Procedure

This paper presents empirical results related to the cybersecurity awareness dimension within a broader study on consumers' functioning in the digital services market. The analytical framework distinguishes five dimensions: technological context, consumer behaviour, consumer competence, consumer protection awareness, and **cybersecurity awareness**. This study focuses exclusively on the last dimension.

The study adopts a quantitative research design aimed at assessing the level of knowledge and awareness of digital threats among Generation Z, with a focus on perceived vulnerability to cybercrime and the assessment of potential harm. The measurement instrument was developed based on a literature review. To capture these dimensions, respondents were asked the following questions:

- [CP1] Indicate how vulnerable do you feel to cybercrime (hacking, viruses, phishing, computer fraud)
- [CP2] How serious do you think the potential harm of cybercrime is?
- [CP3] Determine how vulnerable you feel to having your personal data taken over by criminals.
- [CP4] How serious do you think the potential harm of intercepting personal data is?

Respondents evaluated each statement using a 10-point Likert-type scale, interpreted as a simplified percentage scale, where 0 corresponds to 0% and 10 to values approaching 100%. Intermediate values represent increasing probability levels. The questionnaire also included sociodemographic variables used as grouping factors in further analyses (Table 2).

Data were collected using the CAWI method among Generation Z respondents (born in the late 1990s and early 2000s). A pilot survey conducted in October 2024 confirmed the clarity of the instrument. The main data collection took place between December 2024 and January 2026. After data cleaning, the final sample consisted of 770 valid observations. Participation was voluntary and anonymous. The characteristics of the respondents are presented in Table 2.

Table 2: Sample characteristics

Category	n	%
Gender: male \ female \ other or no answer	292 \ 472 \ 6	37.9 \ 61.3 \ 0.8
Place of residence: large city \ city \ town \ rural area	104 \ 498 \ 79 \ 89	13.5 \ 64.7 \ 10.3 \ 11.6
Professional status: Student (not employed) \ Working student	314 \ 456	40.8 \ 59.2
Level of education: higher education \ secondary education	385 \ 385	50.0 \ 50.0
Financial situation: very good \ good \ neither good nor bad \ rather bad \ very bad	150 \ 438 \ 145 \ 35 \ 2	19.5 \ 56.9 \ 18.8 \ 4.5 \ 0.3

The empirical analysis presented in the following section addresses the research questions formulated for the cybersecurity dimension of the study, with particular emphasis on consumers' perceived vulnerability to cyber threats and their assessment of the potential harm associated with such risks.

4. Results

4.1 Differences in Perceived Vulnerability and Severity

To address **RQ1**, descriptive statistics were used to assess respondents' perceptions of vulnerability to cyber threats and their potential consequences. The results are presented in Table 3.

Table 3: General assessment of perceived vulnerability and potential harm of cyber threats

Variable	Mean (M)	Median	Min	Max	Std.Dev.	St.Err	Skewness	Kurtosis
CP1	5.03	5	1	10	2.288	0.082	0.170	-0.790
CP2	8.31	9	2	10	1.812	0.065	-1.226	1.182
CP3	5.88	6	1	10	2.421	0.087	-0.070	-0.885
CP4	8.45	9	1	10	1.916	0.069	-1.284	0.986

The results presented in Table 3 indicate a clear pattern in the perception of cybersecurity risks. Respondents assess their vulnerability to cyber threats as moderate (CP1: M = 5.03; CP3: M = 5.88), while the perceived severity of potential harm is significantly higher (CP2: M = 8.31; CP4: M = 8.45). This suggests that although respondents do not perceive themselves as highly exposed to cyber threats, they clearly recognize the serious consequences of such incidents. The negative skewness for severity variables confirms a concentration of responses at the higher end of the scale, whereas greater variability is observed for vulnerability assessments. Overall, the findings reveal a discrepancy between perceived vulnerability and perceived severity, indicating a differentiated awareness of cybersecurity risks among Generation Z respondents.

4.2 Perceived Vulnerability to Cybercrime: A Detailed Analysis

The perception of vulnerability to cybercrime may vary across socio-demographic groups. The Kolmogorov–Smirnov test ($D = 0.12$; $p < 0.01$, Lilliefors correction) indicated that the distribution significantly deviates from normality. Therefore, to address **RQ2** and test hypotheses **H2a–H2e**, non-parametric tests were applied.

The Mann–Whitney U test was used for gender (males and females, representing 99.2% of the sample), level of education, and professional status, while the Kruskal–Wallis H test was applied for variables with more than two categories (place of residence and financial situation). The significance level was set at $\alpha = 0.05$, with post hoc analyses conducted where applicable. The results are presented in Tables 4 and 5.

Table 4: The Mann-Whitney U test results

Variable	Z	p-value	Related hypothesis
Gender	-4.991	<0.05	H2a
Level of education	-3.190	<0.05	H2b
Professional status	5.579	<0.05	H2c

Table 5: The Kruskal-Wallis test results

Variable	Results	Related hypothesis
Place of residence	H (3, N= 770) =8.164397 p =0.0427	H2d
Financial situation	H (4, N= 770) =1.383909 p =0.8470	H2e

The Mann–Whitney U test results (Table 4) indicate statistically significant differences by gender ($Z = -4.991$; $p < 0.05$), level of education ($Z = -3.190$; $p < 0.05$), and professional status ($Z = 5.579$; $p < 0.05$), supporting hypotheses H2a–H2c. This suggests that these factors influence respondents' perceived vulnerability to cybercrime. The Kruskal–Wallis test (Table 5) also revealed significant differences by place of residence ($H(3, N$

= 770) = 8.164; $p = 0.0427$), supporting H2d. Post hoc analysis (Dunn's test with Bonferroni correction) showed differences between city and large city ($p = 0.011$) and between large city and town ($p = 0.025$), while other comparisons were not significant. No significant differences were found for financial situation ($H(4, N = 770) = 1.384$; $p = 0.8470$), leading to the rejection of H2e. These results partially confirm the hypotheses, indicating that perceived vulnerability to cybercrime varies across selected socio-demographic variables, particularly those related to social position and experience, while financial situation does not appear to be a significant factor.

To complement the statistical analysis and provide additional insight into RQ2, frequency distributions are presented in Figures 1 and 2.

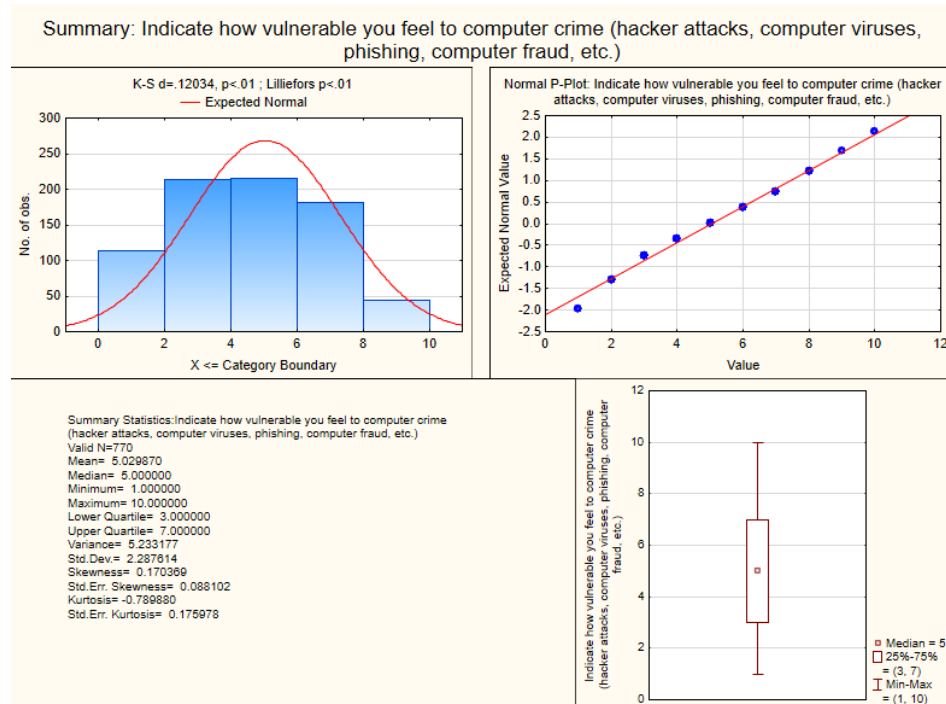


Figure 1: Perceived vulnerability to cybercrime among Generation Z

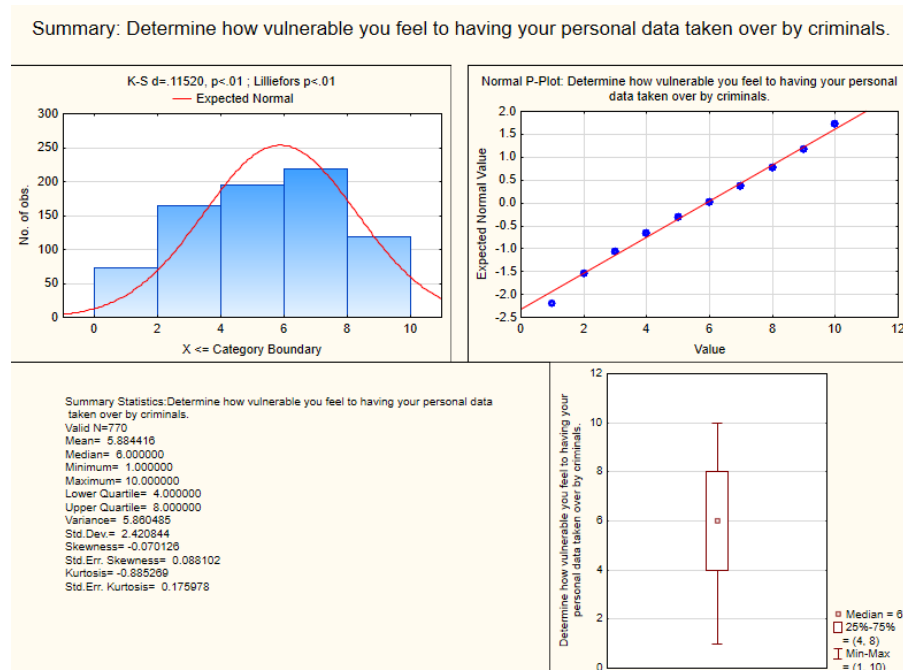


Figure 2: Perceived vulnerability to personal data interception among Generation Z

Figures 1 and 2 present the distributions of respondents' perceived vulnerability to cybercrime and personal data interception. In both cases, the distributions are relatively balanced, with a concentration around the mid-range of the scale, indicating a moderate level of perceived exposure. However, respondents assess vulnerability to personal data interception (CP3) as slightly higher than to cybercrime in general (CP1), which is reflected in a shift toward higher values. Both distributions show noticeable variability, suggesting heterogeneity in risk perception among respondents. A slight skewness is observed, indicating a tendency toward lower values for cybercrime vulnerability and toward higher values for personal data-related threats. Taken together, the results indicate a moderate but differentiated perception of vulnerability, with greater sensitivity to threats directly related to personal data.

4.3 Perceived Severity of Cybercrime: A Detailed Analysis

The perception of the severity of cybercrime consequences may vary across different socio-demographic groups. The Kolmogorov–Smirnov's test results ($D = 0.187$; $p < 0.01$, Lilliefors correction) indicated that the distribution significantly deviates from normality. Therefore, the same analytical procedure as described in Section 4.2 was applied to test hypotheses **H3a–H3e**. The results are presented in Tables 6 and 7.

Table 6: The Mann-Whitney U test results

Variable	Z	p-value	Related hypothesis
Gender	1.890	0.058	H3a
Level of education	2.144	0.031	H3b
Professional status	-1.226	0.219	H3c

Table 7: The Kruskal-Wallis test results

Variable	Results	Related hypothesis
Place of residence	H (3, N= 770) =0.9350351 p =0.8170	H3d
Financial situation	H (4, N= 770) =2.423962 p =0.6583	H3e

The results of the non-parametric tests indicate limited differentiation in the perception of the severity of cybercrime (CP2) across socio-demographic characteristics. The Mann–Whitney U test (Table 6) shows a statistically significant difference only for level of education ($Z = 2.144$; $p = 0.031$), supporting **H3b**. No significant differences were found for gender ($Z = 1.890$; $p = 0.058$) or professional status, leading to the rejection of **H3a** and **H3c**. The Kruskal–Wallis test (Table 7) also revealed no significant differences for place of residence or financial situation, resulting in the rejection of **H3d** and **H3e**. The perception of cybercrime severity appears relatively uniform across the analysed groups, in contrast to perceived vulnerability (CP1), which shows greater differentiation. These findings suggest a consistent assessment of the seriousness of cyber threats among respondents. To complement the statistical analysis and provide additional insight into RQ3, frequency distributions are presented in Figures 3 and 4.

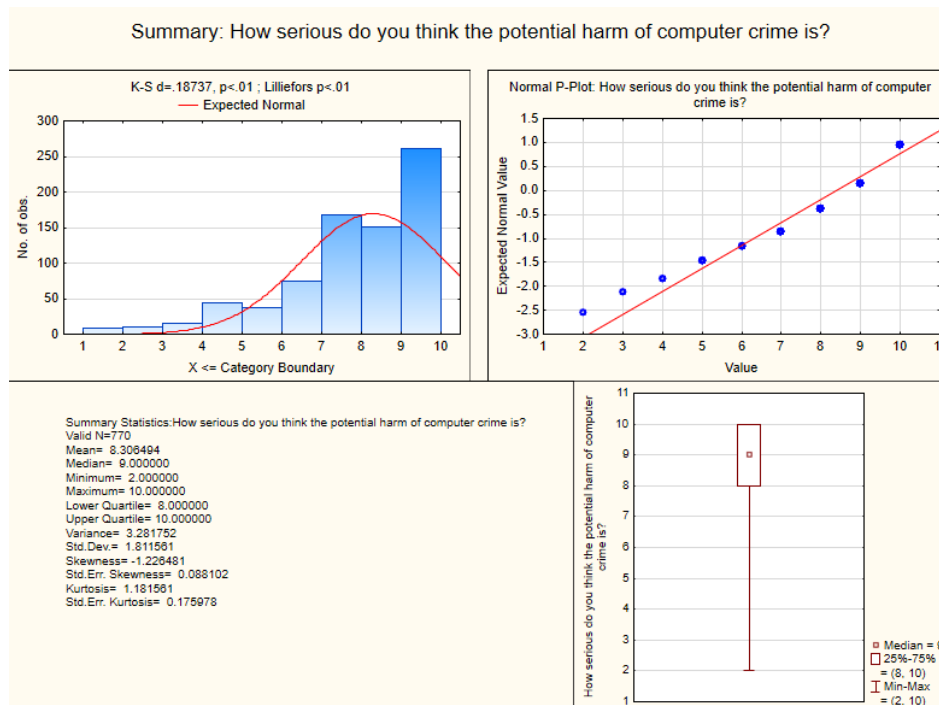


Figure 3: Distribution of perceived severity of cybercrime among Generation Z

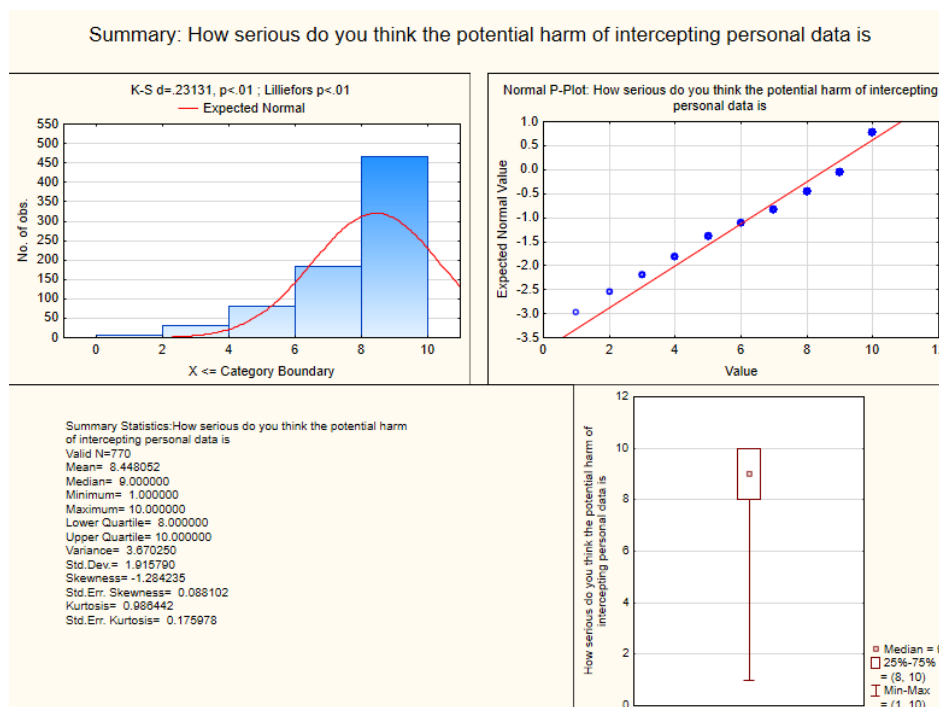


Figure 4: Distribution of perceived severity of personal data interception among Generation Z

Figures 3 and 4 present the distributions of respondents' assessments of the potential harm associated with cybercrime and personal data interception. In both cases, responses are strongly concentrated at the upper end of the scale (8–10), indicating that respondents perceive the consequences of these threats as highly severe.

The distributions are negatively skewed, reflecting a clustering of responses toward higher values and a high level of consensus among respondents. Only a small proportion of responses fall within the lower range, suggesting that cyber threats are rarely perceived as low-risk in terms of their consequences.

Compared to perceived vulnerability, the assessment of potential harm is both higher and more uniform, highlighting a clear asymmetry between perceived exposure and perceived severity. Notably, the perceived

harm of personal data interception (CP4) is slightly higher and more concentrated than that of cybercrime in general (CP2), indicating greater sensitivity to threats directly related to personal data.

5. Discussion and Implication

The study findings provide important insights into the structure of cybersecurity awareness among Generation Z, particularly regarding the asymmetry between perceived vulnerability and perceived severity of digital threats.

Previous research has emphasized that users often constitute the weakest link in cybersecurity systems due to limited awareness and cognitive biases (Heartfield & Loukas, 2015; Basit et al., 2021). The results of this study partially support this view. While respondents demonstrate a high awareness of the potential consequences of cyber threats, their perceived vulnerability remains only moderate. This suggests that the limitation may not lie in the understanding of risk severity, but rather in the personal internalization of exposure.

This finding is consistent with earlier studies indicating that frequent use of digital technologies does not necessarily translate into adequate awareness or responsible behaviour among Generation Z (Fandrejewska et al., 2025). Although young users are highly active in digital environments, they may underestimate their own susceptibility to cyber threats, which can lead to insufficient protective behaviour.

The observed asymmetry between perceived vulnerability and perceived severity may also be interpreted in the context of cognitive biases, such as optimism bias, where individuals tend to believe that negative events are less likely to affect them personally. While previous literature has pointed to the importance of risk perception in shaping cybersecurity behaviour, this study highlights that the two dimensions of risk, probability and consequences, are not necessarily aligned. At the same time, the results indicate that perceived severity of cyber threats is relatively uniform across socio-demographic groups, whereas perceived vulnerability shows greater differentiation. This suggests that awareness of the seriousness of cyber threats is widely shared, whereas perceptions of personal exposure are more dependent on individual characteristics such as gender, education, or professional status. This partially aligns with prior research emphasizing the role of individual differences in cybersecurity awareness and behaviour.

To sum up, the findings contribute to the existing literature by demonstrating that cybersecurity awareness among Generation Z is not homogeneous but structured, with a clear imbalance between the perception of risk severity and personal vulnerability. This has important implications for the design of educational and awareness-raising initiatives, which should focus not only on communicating the consequences of cyber threats but also on strengthening individuals' perception of their own exposure to risk.

6. Limitations and Future Research

This study has several limitations. The sample is limited to Generation Z, which restricts generalizability. The use of self-reported measures may introduce bias, as perceived vulnerability and severity do not necessarily reflect actual behaviour. Future research could include more diverse age groups, apply longitudinal approaches, and incorporate behavioural or experimental measures to better capture cybersecurity practices, as well as explore these relationships across different contexts.

Ethics Declaration: The author declares that there are no conflicts of interest related to this study. Participation in the survey was voluntary, and informed consent was obtained from all respondents. The data were collected anonymously and used exclusively for research purposes.

AI Declaration: Artificial intelligence (AI) tools were used to support language editing and improve the clarity of the manuscript. The author takes full responsibility for the content, analysis, and interpretation of the results.

References

- Al-Muwil, A., Weerakkody, V., El-Haddadeh, R., & others. (2019). Balancing digital-by-default with inclusion: A study of the factors influencing e-inclusion in the UK. *Information Systems Frontiers*, 21(3), 635–659.
<https://doi.org/10.1007/s10796-019-09914-0>
- Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 12, 30907–30927.
<https://doi.org/10.1109/ACCESS.2024.3369906>
- Aslan, O., & Samet, R. (2019). A comprehensive review on malware detection approaches. *IEEE Access*, 8, 6249–6271.
<https://doi.org/10.1109/ACCESS.2019.2963724>

- Basit, A., Zafar, M., Liu, X., & others. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76, 139–154. <https://doi.org/10.1007/s11235-020-00733-2>
- Bochyńska, A. (2026, April 8). *Cyberatak co dwie minuty: Nowy raport CERT Polska nie pozostawia złudzeń [A cyberattack every two minutes: The new CERT Polska report leaves no doubt]*. WNP.pl. <https://www.wnp.pl/tech/cyberatak-co-dwie-minuty-nowy-raport-cert-polska-nie-pozostawia-zludzen,1050224.html>
- CBZP. (2025, September 5). *Ponad 1,5 tys. oszukanych metodą na wyludzanie kodów płatności*. Retrieved April 8, 2026, from <https://cbzc.policja.gov.pl/bzc/aktualnosci/676,Ponad-15-tys-oszukanych-metoda-na-wyludzanie-kodow-platnosci-Kolejni-podejrzani-w-rekach-cyberpolicjantow.html>
- Cisco. (2025). *Cisco cybersecurity readiness index 2025: Poland*. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index_PL.pdf
- Cosgrove, J. & Cachia, A. R. (2025). *DigComp 3.0: European Digital Competence Framework - Fifth Edition*. Publications Office of the European Union, Luxembourg. <https://data.europa.eu/doi/10.2760/0001149>
- Fandrejewska, A., Eisenhardt, M., & Eisenhardt, T. (2025). Generation Z's Perception of Knowledge and Learning in the Context of Formal and Informal Education. *Procedia Computer Science*, 270, 1272–1281. <https://doi.org/10.1016/j.procs.2025.09.248>
- Fandrejewska-Nowakowska, A., Eisenhardt, M., & Eisenhardt, T. (in press). *Consumer behavior and digital services: Competence, rights and protection*. Taylor & Francis.
- Government of Poland. (n.d.). *Cyberbezpieczeństwo w małej i średniej firmie*. Retrieved April 8, 2026, from <https://www.biznes.gov.pl/pl/portal/004175>
- Greser, J. (2021). Cyberbezpieczeństwo a uczestnictwo MŚP w jednolitym rynku cyfrowym. In K. Kokocińska (Ed.), *Publicznoprawne aspekty udziału sektora MŚP w procesie realizacji strategicznych celów polityki rozwoju [Public law aspects of SME participation in the implementation of strategic development policy goals]* (pp. 103–123). Poznań, Poland: Wydawnictwo UAM.
- Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3). <https://doi.org/10.1145/2835375>
- Lastdrager, E. E. (2014). Achieving a consensual definition of phishing based on a systematic review of the literature. *Crime Science*, 3(9). <https://doi.org/10.1186/s40163-014-0009-y>
- Lipińska, M., Kotula, N., & Jemielniak, D. (2025). Exploring expert figures in alien-related UFO conspiracy theories. *Humanities and Social Sciences Communications*, 12, 535. <https://doi.org/10.1057/s41599-025-04799-8>
- Mahmoudi, A., Jemielniak, D., & Ciechanowski, L. (2024). Echo chambers in online social networks: A systematic literature review. *IEEE Access*, 12, 9594–9620. <https://doi.org/10.1109/ACCESS.2024.3353054>
- Mahmoudi, A., Jemielniak, D., & Ciechanowski, L. (2025). Characteristics of two polarized groups in online social networks' controversial discourse. *Journal of Computational Social Science*, 8, 22. <https://doi.org/10.1007/s42001-024-00350-y>
- NASK. (2024). *300 incydentów dziennie – premiera raportu CERT Polska za 2024 rok [300 incidents per day – release of the CERT Polska report for 2024]*. Retrieved April 8, 2026, from <https://www.nask.pl/aktualnosci/300-incydentow-dziennie-premiera-raportu-cert-polska-za-2024-rok>
- Nowak, W. (2020). Specyfika zagrożeń w cyberprzestrzeni. In C. Banasiński & M. Rojszczak (Eds.), *Cyberbezpieczeństwo*. Warsaw, Poland.
- Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era: A state-of-the-art survey. *ACM Computing Surveys*, 52(5). <https://doi.org/10.1145/3329786>
- PDP UW. (2026). *Zasady cyberhigieny*. University of Warsaw & Office for Personal Data Protection. <https://odo.uw.edu.pl/wp-content/uploads/sites/10/2026/02/poradnik-zasady-cyberhigieny.pdf>
- CERT Polska. (2025). *Raport roczny 2024 z działalności CERT Polska: Krajobraz bezpieczeństwa polskiego internetu [Annual report 2024 of CERT Polska: The Polish internet security landscape]*. Retrieved from https://cert.pl/uploads/docs/Raport_CP_2024.pdf
- CERT Polska. (2026). *Raport roczny 2025 z działalności CERT Polska: Krajobraz bezpieczeństwa polskiego internetu [Annual report 2025 of CERT Polska: The Polish internet security landscape]*. Retrieved from https://cert.pl/uploads/docs/Raport_CP_2025.pdf
- Sanders, C. K., & Scanlon, E. (2021). The digital divide is a human rights issue: Advancing social inclusion through social work advocacy. *Journal of Human Rights and Social Work*, 6, 130–143. <https://doi.org/10.1007/s41134-020-00147-9>
- Schabikowska, A. (2025, August 22). *Współczesne ataki cybernetyczne: Jak zmieniają się metody przestępców? Exorigo-Upos*. Retrieved April 8, 2026, from <https://www.exorigo-upos.pl/blog/wspolczesne-ataki-cybernetyczne-nowe-metody-przestepcow/>
- Urbanek, W. (2024, September 2). *Cyberatak z wnętrza firmy*. Businessman.pl. Retrieved April 8, 2026, from <https://businessman.pl/artykuly/cyberatak-z-wnetrza-firmy>
- Vassilakopoulou, P., & Hustad, E. (2023). Bridging digital divides: A literature review and research agenda for information systems research. *Information Systems Frontiers*, 25, 955–969. <https://doi.org/10.1007/s10796-020-10096-3>
- Wolny, R. (2020). Świadomość istnienia niebezpieczeństw korzystania z e-usług wśród młodych konsumentów. In B. Mróz (Ed.), *Bezpieczeństwo konsumentów na rynku tradycyjnym i wirtualnym [Consumer safety in traditional and virtual markets]* (pp. 89–100). Warsaw, Poland: Oficyna Wydawnicza SGH.