SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 241

GENDER DIFFERENCES IN PERCEPTION AND BEHAVIOR TOWARDS CYBER THREATS – RESEARCH RESULTS AMONG FINANCIAL SERVICES USERS IN POLAND

Jagoda ŻUREK[1*], Rafał PITERA[2]

[1] University of Rzeszów, Faculty of Economics and Finance; jzurek@ur.edu.pl, ORCID: 0000-0002-2659-8026
[2] University of Rzeszów, Faculty of Economics and Finance; rpitera@ur.edu.pl, ORCID: 0000-0001-9598-1240
* Correspondence author

Purpose: This study aims gender differences in the perception of cyberthreats and cybersecurity behaviours among users of financial services in Poland. The paper seeks to determine whether men and women differ in their attitudes, risk assessment, and protective practices in the context of rapidly expanding digital banking and online financial services.
Design/methodology/approach: The research was conducted using the CAWI method on a sample of Polish users of financial services. Statistical analyses included the Pearson's chi-square test and the Mann–Whitney U test, allowing the identification of significant gender-based differences in the perception of cyberthreats and cybersecurity behaviours.
Findings: The results show that although men and women assess their knowledge of cyberthreats similarly, their practical behaviours differ. Women are more likely to apply additional security measures—such as complex passwords, biometric authentication, and two-factor authentication—and to regularly monitor their bank accounts. Men tend to express a higher sense of digital security. Differences were also observed in the perceived responsibility of institutions for ensuring cybersecurity.
Research limitations/implications: The study is limited by the use of self-reported data and a non-probabilistic sampling method. Future research could expand the sample, include behavioural tracking measures, or compare findings across countries.
Practical implications: The findings indicate the need to differentiate educational and communication strategies in cybersecurity. Financial institutions and public agencies should tailor training materials and awareness campaigns to gender-specific behavioural patterns.
Social implications: By highlighting gender-related differences in cybersecurity practices, the study supports initiatives aimed at improving digital safety and reducing exposure to cyber threats. The results may inform public policy and contribute to more effective national cybersecurity education programmes.
Originality/value: This study provides one of the few empirical analyses of gender differences in cybersecurity behaviour specifically within the context of financial services in Poland. It offers new insights for researchers, practitioners, and policymakers by combining perception-based and behaviour-based measures of cybersecurity.
Keywords: cybersecurity, gender differences, cyberthreats, financial services users, digital safety.
Category of the paper: Research paper.
JEL Code: D83, D91, G21.

1. Introduction

In an era of intense digitization of the economy and society, cybersecurity issues have become crucial for both individuals and public and private institutions. The dynamic development of information and communication technologies (ICT) and the growing popularity of online banking, social media, and e-commerce mean that internet users are increasingly exposed to cyber threats. According to a report by the European Union Agency for Cybersecurity (ENISA, 2024), as many as 84% of internet users in EU countries have experienced at least one cybersecurity incident in the last three years. In this context, it is crucial to understand how different social groups – including women and men – perceive the risk of cyber threats, what protective strategies they employ, and how they respond to data breaches.

Cybersecurity is defined as "the ability to protect information systems, networks, and data from cyberattacks, their unauthorized use, damage, or destruction" (Kuzior et al., 2024). The literature emphasizes that the effectiveness of cybersecurity depends not only on technology but also on the human factor – knowledge, awareness, and behavior of users (Metalidou et al., 2014). For this reason, research on behavioral aspects of cybersecurity is gaining importance, combining IT with psychological, sociological, and economic perspectives.

Previous studies on online user behavior have repeatedly highlighted the importance of gender differences in the use of digital technologies, risk assessment, and response to threats (Cele, Kwenda, 2023; Sulaiman et al., 2022). Women are more likely to be cautious and more prone to following security rules, while men demonstrate greater confidence in using digital tools but are also more likely to engage in risky behavior online (Alrababah, Iqbal, Khan, 2024). These differences stem from both social factors (e.g., stereotypes regarding technological competence) and psychological factors (e.g., different levels of risk perception, emotional reactions, and motivation to learn cybersecurity principles). From an economic and organizational perspective, understanding these differences has practical implications. Knowledge about the different behavioral patterns of women and men can help financial institutions, public administration, and technology companies design more effective educational strategies, information campaigns, and digital security training programs. International research findings (including the Global Cybersecurity Index and ITU 2023) show that countries with higher levels of public awareness of cybersecurity experience fewer incidents involving individual users. In this context, examining gender differences can provide valuable information on areas that require specific educational support.

In Poland, as in many other European countries, there is an increase in the number of cyber incidents affecting both individual users and businesses. Data from CERT Polska (2024) shows that the most common threats are phishing, social engineering attacks, login credentials theft, and malware installed on mobile devices. With the development of online banking and mobile

payments, user trust in the digital environment is becoming increasingly important. Research indicates that women are more likely than men to express concerns about losing financial data, while men are more likely to downplay the risk (Al Doghan, 2024). Such differences may affect not only the level of individual security but also the rate of adoption of modern financial technologies, such as mobile payments or investment apps.

The aim of this article is to identify and analyze gender differences in the perception and behavior toward cyberthreats among financial services users in Poland. In an era of dynamic development of digital technologies, this issue is particularly important from the perspective of both financial science and digital security. Analyzing gender differences in risk perception, security measures used, and responses to digital threats will allow for a better understanding of the factors determining user behavior in the online environment. The obtained results contribute to the development of knowledge about the social determinants of cybersecurity and can serve as a basis for practical recommendations for financial institutions and public policymakers.

The originality of this study lies in its empirical focus on gender differences in both the perception of cyberthreats and actual cybersecurity behaviours among financial services users in Poland. Unlike many previous studies that concentrate primarily on technological aspects of cybersecurity or on general internet use, this research combines perception-based and behaviour-based measures within the specific context of digital financial services. By addressing a nationally specific yet underexplored setting, the study fills a gap in the literature and contributes empirical evidence relevant for both academic research and practical cybersecurity policy.

2. Methods

The study was conducted using an online survey (CAWI) on a sample of 1539 financial service users, including 864 women (56.1%) and 675 men (43.9%). Financial service users were defined as those using online banking and other forms of digital financial services. Respondents represented a variety of age groups, education levels, and places of residence. The largest group were participants aged 18-24 (45.4%), while those over 55 constituted 19.5% of the sample. The majority of respondents had higher education (52.4%) or secondary education (46.4%). Nearly half of the respondents lived in rural areas (45.8%), and 23% lived in cities with populations between 50,000 and 100,000. Household income per person was most often in the range of PLN 4001-6000 (25.7%) or above PLN 6000 (25%). Most households had two (34.7%) or four (26.1%) people. The study was conducted on a non-randomly selected sample.

The following research hypotheses were formulated in this study:

H1: Men rate their knowledge of cyber threats in online banking higher than women.

H2: Women demonstrate a higher level of concern about cyber threats than men.

H3: Men are more likely than women to report feeling safe when using online banking.

H4: Men are more likely than women to trust non-bank financial institutions.

H5: Indications regarding industries perceived as leaders in cybersecurity differ by gender – men are more likely to choose banks and fintech companies, while women are more likely to choose service institutions (e.g., public administration, online payment operators).

H6: Men are more likely than women to use technological security measures (e.g., biometrics, 2FA), while women are more likely to follow precautionary measures (e.g., regularly changing passwords).

H7: Men are more likely than women to use the same passwords across different services.

H8: Women are more likely than men to regularly monitor their bank accounts to detect unauthorized transactions.

Statistical analysis methods appropriate for qualitative and ordinal data were used to verify the hypotheses. The Mann-Whitney U test was used to assess differences between two independent groups. This is a nonparametric statistical test used when the dependent variable is ordinal or when the data distribution deviates from normality, thus not meeting the assumptions of parametric tests (Moczko, Bręborowicz, Tadeusiewicz, 2013). The test analyzes the ranks of observations assigned to both groups, assessing whether there are significant differences between them. Results are presented using the U statistic, which is then converted to a p-value to determine statistical significance (Chicco, Sichenze, Jurman, 2025). The chi-square test of independence (χ^2) and Cramér's V coefficient, which allows for determining the strength of the relationship between the analyzed characteristics, were used to examine the relationships between qualitative variables (Wiktorowicz, Grzelak, Grzeszkiewicz-Radulska, 2020). A significance level of $p < 0.05$ was used in all analyses.

The V coefficient values were interpreted according to the following criteria: 0.10 indicates a weak relationship, 0.30 indicates a moderate relationship, and 0.50 indicates a strong relationship. This coefficient ranges from 0 to 1, regardless of the number of categories in the contingency table (Prajzner, 2022; Wiktorowicz, Grzelak, Grzeszkiewicz-Radulska, 2020). The tables also provide degrees of freedom (df), determined based on the number of categories in the variables analyzed.

3. Results and discussion

This section of the article presents the results of an analysis of differences between women and men in their perceptions and behaviors toward cyberthreats in the context of using e-banking and digital financial services. The analysis encompassed subjective assessments of knowledge about digital threats, levels of concern and trust in financial institutions, and practices for securing bank accounts. The results are presented in the order of the research hypotheses.

Table 1 presents the results of the analysis of differences in self-assessed knowledge of cyber threats in e-banking by gender. The results of the Mann-Whitney U test did not reveal statistically significant differences between women and men (U = 279634.5; p = 0.102). The mean rank for women (783.85) was slightly higher than for men (752.27), which may indicate that women report a slightly higher level of knowledge, but this difference remains statistically insignificant. This indicates that the level of subjective knowledge of digital threats is comparable between both genders. Consequently, hypothesis H1, which assumed that men rate their knowledge of cyber threats higher than women, was not supported.

Table 1.
Gender differences in self-assessment of knowledge about cyber threats

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
Self-assessment of knowledge about cyber threats	279634.5	752.27	783.85	0.102

Source: Own work.

The obtained results are consistent with some previous studies indicating a lack of significant gender differences in perceived cybersecurity competence or behaviors. For example, Branley-Bell et al. (2022) found that gender was not a significant predictor of information security behaviors in a study that included practices such as password generation, device security, and software updates (n = 579), which may support the thesis of a systematic reduction in gender differences in this area, resulting, among other things, from similar levels of exposure to digital technologies.

Table 2 presents the results of the analysis of differences in the level of concern about cyber threats related to e-banking by gender. The results of the Mann-Whitney U test revealed no significant differences between women and men (U = 280881.0; p = 0.2008). The mean rank of women (782.41) was higher than that of men (754.12), which may indicate a slightly higher level of concern among women, but this difference remains statistically insignificant. Therefore, hypothesis H2, according to which women demonstrate a higher level of concern about cyber threats than men, was not confirmed.

Table 2.
Gender differences in the level of concern about cyber threats in e-banking

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
Level of concern about cyber threats	280881.0	754.12	782.41	0.2008

Source: Own work.

The literature finds evidence that women are more likely than men to report higher levels of concern or risk perception in the digital space (Stevens et al., 2024). McGill and Thompson (2018) also indicate that although women perceive the effects of potential security incidents as more severe (higher perceived severity), they do not feel more vulnerable to such threats than men. In light of these studies, the result of our study—the lack of a significant gender difference in the level of concern—may suggest that in the context of e-banking, both genders have similar risk perceptions, and the specific nature of e-financial services may partially offset the differences observed in other areas of digital activity.

Table 3 presents the results of the analysis of differences in the sense of security when using e-banking by gender. The question was rated on a five-point scale (1 – I definitely do not feel safe, 5 – I definitely feel safe). The results of the Mann-Whitney U test confirmed the existence of statistically significant differences between women and men ($U = 231{,}435.0$; $p < 0.001$). The mean rank of men (680.87) was lower than that of women (839.64), which – considering the direction of the scale – means that men were more likely to report a higher level of security when using e-banking. Therefore, hypothesis H3, which assumed that men were more likely than women to report feeling secure in the e-banking environment, was confirmed.

Table 3.
Gender differences in the sense of security when using e-banking

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
A sense of security against cyber threats	231435.0	680.87	839.64	<0,001*

Source: Own work.

Interpretation of these results indicates that men are more likely to report a high sense of security when using online banking, which may be associated with a higher level of technological confidence. However, a higher sense of security does not necessarily reflect a true level of preparedness to cope with cyberthreats. This phenomenon is confirmed by the results of Polish population studies (Warsaw Institute of Banking, 2025), in which men more often indicated that they felt safe in the digital environment, despite simultaneously being aware of numerous threats related to using the internet and social media. This study also noted that residents of large cities aged 45+ more often reported a higher sense of security, while education level did not differentiate this indicator.

The results of this study suggest a discrepancy between risk assessment and a sense of security in women and men. Although both groups perceive digital threats similarly, women are significantly more likely to feel less safe in the online banking environment. This may be due to differences in the subjective sense of control over the security of digital services, rather than actual levels of knowledge or experience. At the same time, women's higher caution may

have a protective effect, while men's greater self-confidence—if not accompanied by appropriate vigilance—may increase their vulnerability to security incidents.

Table 4 presents the results of the analysis of differences in the level of trust in non-bank financial institutions regarding cybersecurity by gender. Responses were rated on a five-point scale (1 – I strongly distrust, 5 – I strongly trust). The results of the Mann-Whitney U test indicate statistically significant differences between women and men ($U = 220918.5$; $p < 0.001$). The mean rank of women (851.81) was higher than that of men (665.29), which – considering the direction of the scale – means that women were more likely to declare a higher level of trust in non-bank financial institutions. Hypothesis H4 (men are more likely than women to trust non-bank financial institutions) was therefore not confirmed.

Table 4.
Gender differences in the level of trust in non-bank financial institutions in terms of cybersecurity

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
Trust in non-bank financial institutions	231435.0	680.87	839.64	<0,001*

* $p < 0,05$ – statistically significant results.

Source: Own work.

The obtained results indicate that women in the study sample declared a significantly higher level of trust in non-bank financial institutions than men, which contradicts some previous research. The literature on fintech and digital financial services often emphasizes that women are more cautious, more likely to be concerned about security issues, and less likely to use innovative financial solutions. For example, Chen (2023) describes the so-called "fintech gender gap," indicating that women are less likely than men to use fintech services due, among other reasons, to greater concerns about privacy and security. Similarly, Sikakebieke and Kuanova (2025) demonstrated that women in emerging markets are characterized by a lower propensity to adopt digital financial services and a lower level of trust in them.

At the same time, other studies demonstrate that gender differences in trust are not clear-cut and may depend on context. Sholevar and Bachmann (2025) emphasize that gender alone does not determine the level of trust in financial services. Meanwhile, the results of Yadav et al. (2024) show that women's trust in digital services increases when solutions are perceived as safe, intuitive, and user-friendly.

Considering these results, the fact that women in the study sample are more likely to trust non-bank financial institutions than men may suggest that, in the Polish digital services market, traditional gender differences in perceived security are gradually weakening, or even partially reversing. It is possible that the transparency of interfaces, communication emphasizing security, and positive user experiences lead women to perceive such entities as more trustworthy. At the same time, the results suggest that trust-building strategies in the financial environment should take into account the different security expectations of women and men and their different sensitivity to risk factors.

Table 5 presents the results of the analysis of the relationship between respondents' gender and the perception of various industries and institutions as cybersecurity leaders. The Pearson χ^2 test revealed statistically significant differences ($p < 0.05$) in eight of the nine analyzed categories. This indicates that the perception of cybersecurity leaders varied depending on the respondents' gender. The obtained Cramér's V coefficient values ranged from 0.035 to 0.233, indicating that the relationship between respondents' gender and the perception of specific industries as cybersecurity leaders is weak.

The strongest relationships were observed for online payment operators (V = 0.231) and insurance companies (V = 0.233), where the correlation reached a moderate level. For other categories—such as banks, technology companies, public administration, telecommunications companies, shopping platforms, and fintech companies—V values ranged from 0.056 to 0.108, indicating weak relationships. The lowest coefficient value was observed in the "other" category (V = 0.035), where no statistically significant differences were found.

Table 5.
The relationship between gender and the industry perceived as a leader in cybersecurity

Industry / institution	χ^2	df	V	p-value
Banks	18.06	1	0.108	< 0.001*
Technology companies	5.19	1	0.058	0.0227*
Public administration	8.29	1	0.073	0.004*
Telecommunications companies	7.74	1	0.071	0.0054*
Online payment operators	82.26	1	0.231	< 0.001*
Insurance institutions	83.45	1	0.233	< 0.001*
Shopping platforms	4.78	1	0.056	0.0288*
Fintechs	12.87	1	0.091	< 0.001*
Other	1.90	1	0.035	0.1678

* $p < 0,05$ – statistically significant results.

Source: Own work.

Table 6 presents the gender breakdown of responses regarding the perception of industries and institutions as leaders in cybersecurity. Men were more likely than women to identify banks (86.7% and 78.1%, respectively), and fintech companies (13.3% and 7.6%). Women, on the other hand, were more likely to identify technology companies (27.4% vs. 22.2%), public administration (12.2% vs. 7.6%), telecommunications companies (1.4% vs. 0%), online payment operators (34.7% vs. 14.2%), insurance institutions (11.8% vs. 0%), and shopping platforms (8.3% vs. 5.3%). In the "other" category, the percentage of responses was negligible in both groups (<1%).

Table 6.
Structure of responses by gender regarding the perception of industries and institutions as leaders in the field of cybersecurity (in %)

Industry / institution	Women (%)	Men (%)
Banks	78.1	86.7
Technology companies	27.4	22.2
Public administration	12.2	7.6
Telecommunications companies	1.4	0.0
Online payment operators	34.7	14.2
Insurance institutions	11.8	0.0
Shopping platforms	8.3	5.3
Fintechs	7.6	13.3
Other	0.0	0.4

The question was multiple choice, so the percentages presented in the table do not add up to 100%.

Source: Own work.

These results confirm that women more often associate cybersecurity with consumer and service institutions, while men more often associate it with the financial and technology sectors. This indicates different patterns of digital security perception depending on gender. Hypothesis H5, which assumed that indications regarding industries perceived as leaders in cybersecurity differ by gender, was confirmed.

The results of our study partially correspond to the results of population-based studies conducted in Poland. The Warsaw Institute of Banking (2024), in its report "Cyberbezpieczny Portfolio", conducted on a representative sample of adult Poles, indicates that banks are clearly recognized as leaders in cybersecurity (54% of responses). Technology companies (30%) and uniformed services such as the military (29%) and the police (28%) also rank highly. These results confirm the dominant position of banks in the public consciousness as entities responsible for cybersecurity.

According to Chen (2023), men are more likely to use fintech services than women, which may contribute to a stronger association of these institutions with digital security. Furthermore, research on the adoption of mobile payments and trust in digital services indicates that women place their trust more heavily on the perceived security and transparency of solutions, as well as on the quality of communication regarding security (Murphy, Tocher, 2011). This may explain why, in this study, women were more likely to identify online payment operators, technology companies, and public administration as leaders in cybersecurity – these institutions are often perceived as responsible for digital infrastructure and for implementing security standards.

Hossain's (2019) study on the adoption of mobile payments found that perceived risk negatively impacts customer trust, and trust is a key factor in building loyalty to mobile services. The author also emphasizes that gender moderates the relationships between perceived security, trust, and the adoption of mobile payments, further indicating that the importance of security may differ between women and men. The results of this study therefore fit into the broader context of literature confirming that trust-building mechanisms in digital services are

gender-specific and may translate into the perception of various industries as cybersecurity leaders.

Table 7 presents the results of the analysis of the relationship between respondents' gender and the methods used to secure access to bank accounts. All analyzed relationships were statistically significant ($p < 0.001$). Cramér's V coefficient values ranged from 0.089 to 0.524, indicating weak to strong relationships. The strongest relationships were observed in the absence of additional security measures ($V = 0.524$) and in the use of two-factor authentication ($V = 0.342$).

Table 7.
The relationship between gender and the use of bank account security methods

Dependent variable	χ^2	df	V	p-value
Using a strong password (a combination of letters, numbers, and special characters)	12.27	1	0.089	< 0.001*
Different passwords for different accounts (e.g. bank, email, social media)	44.23	1	0.17	< 0.001*
Change your password quarterly or more often	37.93	1	0.157	< 0.001*
Two-step verification (SMS code, in-app confirmation)	180.09	1	0.342	< 0.001*
Biometrics (fingerprint, facial recognition)	108.04	1	0.265	< 0.001*
No additional security measures	421.99	1	0.524	< 0.001*

* $p < 0,05$ – statistically significant results.

Source: Own work.

To determine the direction of the relationship, an analysis of the structure of responses by gender was conducted (Table 8). The results indicate that women are more likely than men to declare the use of all analyzed security measures – both traditional (strong passwords, different passwords, regular password changes) and technological (biometrics, two-factor authentication). The lack of additional security measures was significantly more common among men (44.4%) than women (1.7%).

Table 8.
Structure of responses by gender regarding the methods used to secure a bank account (%)

Security method	Women (%)	Men (%)
Strong password (combination of letters, numbers, special characters)	75.3	67.1
Different passwords for different accounts (e.g. bank, email, social media)	37.2	21.3
Change your password quarterly or more often	16.7	6.2
Two-step verification (SMS code, in-app confirmation)	77.1	43.6
Biometrics (fingerprint, facial recognition)	48.6	22.7
No additional security measures	1.7	44.4

The question was multiple choice, so the percentages presented in the table do not add up to 100%.

Source: Own work.

The results suggest that women demonstrate a higher level of concern for bank account security and greater awareness of cybersecurity. Hypothesis H6 (men are more likely than women to use technological security measures, while women are more likely to adhere to precautionary measures) was not confirmed.

The co-occurrence of multiple cybersecurity practices among female respondents suggests the presence of behavioural clustering in digital security strategies. Women simultaneously report significantly higher use of strong and diversified passwords, biometric authentication, and two-factor verification, indicating a more holistic and integrated approach to account protection rather than isolated defensive actions. Although formal cluster analysis was not conducted in this study, the observed pattern of combined safeguards points to the existence of distinct behavioural profiles in cybersecurity practices, which may differentiate users not only by gender but also by their overall security orientation.

A study by Liu et al. (2025) demonstrated that gender influences the use of digital financial services and risk responses, which may explain women's increased vigilance regarding security. Coopamootoo and Ng (2023) indicate that women are more likely than men to use online security advice and are more likely to use security measures. These results are consistent with the findings, which indicate that women are more likely to report using various security measures (strong passwords, 2FA, biometrics). This difference may result from women's higher risk perception or lower technological confidence, which translates into the use of more security measures.

Table 9 presents the results of the analysis of differences between women and men in using the same passwords across various online services, including online banking. The gender differences were statistically significant ($U = 250105.5$; $p < 0.001$). Men's mean rank (831.47) was higher than women's (721.97), indicating that men are more likely than women to use the same passwords across various accounts, such as banks, email, and social media. The results indicate men's lower level of caution when it comes to password management and a greater propensity for risky behaviors related to digital security. Hypothesis H7 (men are more likely than women to use the same passwords across various services) was confirmed.

Table 9.
Gender differences in the use of the same passwords on different websites

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
Using the same passwords on different websites	231435.0	680.87	839.64	<0.001*

* $p < 0,05$ – statistically significant results.

Source: Own work.

The latest survey, "Poles' Attitudes Toward Cybersecurity" (Warsaw Institute of Banking 2025), conducted on a representative sample of adult Poles (n = 1008), revealed a low level of use of password security tools. Only 10% of respondents reported using password generators that create strong, difficult-to-crack combinations. One in three respondents (32%) creates passwords themselves, basing them on their own word associations. However, 19% of respondents – primarily those aged 18-34 – store passwords in a password manager, providing them with a higher level of protection.

Table 10 presents the results of the analysis of differences between women and men in the frequency of monitoring bank accounts to detect unauthorized transactions. The results of the Mann-Whitney U test ($U = 229671.0$; $p < 0.001$) indicate statistically significant differences between the sexes. The question used a five-point scale, with lower scores indicating more frequent bank account monitoring (1 = daily, 5 = no monitoring). The mean score for men (861.75) was higher than for women (698.32), indicating that men monitor their bank accounts less frequently than women.

The results suggest that women are more systematic and vigilant in monitoring financial transactions, which may reflect their higher level of cybersecurity caution. Hypothesis H8 (women are more likely than men to regularly monitor their bank accounts to detect unauthorized transactions) was supported.

An important empirical finding of this study is the perception–behavior gap observed among male respondents. While men report a higher sense of security when using digital financial services, this subjective confidence is not accompanied by corresponding protective behaviours, such as regular account monitoring or diversified password use. This mismatch between perceived safety and actual cybersecurity practices may increase vulnerability to cyber incidents and shows that self-reported feelings of security do not necessarily reflect users' actual level of protection.

Table 10.
Gender differences in bank account monitoring frequency

Variable	U	Mid Rank (Men)	Mid Rank (Women)	p-value
Bank account monitoring frequency	229671.0	861.75	698.32	< 0.001*

* $p < 0,05$ – statistically significant results.

Source: Own work.

In the context of the literature, these findings can be interpreted as part of a broader trend: according to studies by Liu et al. (2025) and Coopamootoo and Ng (2023), women are more likely to take preventative measures and demonstrate greater awareness of digital threats than men. Women are more likely than men to use security advice and more actively implement protective measures regarding digital services. At the same time, Lobão's (2024) study indicates that men tend to overestimate their risk tolerance, which can actually lead to lower risk perception and lower vigilance. Therefore, financial institutions should consider differentiated communication strategies—including incentives and reminders to regularly monitor acccounts—to increase vigilance among all users, especially men.

4. Summary

The study revealed gender differences in cybersecurity behavior in online banking. Although women and men report similar levels of awareness of threats and concern, women are more likely to take preventative measures—using complex and diverse passwords, utilizing two-factor authentication and biometrics, and regularly monitoring their accounts. This indicates a higher level of operational vigilance and awareness of the potential consequences of security incidents. Men, on the other hand, more often report feeling secure when using financial services, although this does not always translate into the implementation of appropriate security measures. The noticeable discrepancy between a high sense of security and a greater propensity for risky behavior may increase their vulnerability to cybersecurity incidents. The results also indicate different trust patterns: men are more likely to perceive banks and fintech companies as security leaders, while women assign a greater role to banks and payment processors. In practice, this suggests the need for differentiated communication approaches.

Based directly on the identified empirical patterns, cybersecurity communication and education strategies should be differentiated by gender. Given men's higher subjective sense of security combined with weaker protective behaviours, interventions targeting male users should prioritize reminders for regular transaction monitoring, warnings against password reuse, and automated alerts. In contrast, women's more frequent use of advanced security measures suggests that educational efforts should focus on reinforcing these behaviours and sustaining engagement with technological safeguards such as biometrics and two-factor authentication. Such targeted approaches may enhance the effectiveness of cybersecurity policies and reduce users' exposure to digital financial risks.

Knowledge about the different behavioral patterns of women and men can support financial institutions, public administration, and the technology sector in more effectively designing targeted educational and communication strategies regarding cybersecurity. Access to tailored messages may contribute to more informed and responsible user behavior in the digital environment, thereby reducing society's vulnerability to cybersecurity incidents.

This study was based on a non-random sample, which limits the generalizability of the results to the entire population of financial services users in Poland. The study also focused on gender, omitting other factors that could significantly differentiate attitudes and behaviors, such as age, education, level of digital literacy, technological experience, and cultural background. Future research would benefit from a multidimensional approach and the inclusion of behavioural data, allowing for a more comprehensive assessment of cybersecurity practices in real-world settings.

References

1. Al Doghan, M.A. (2024). Cybersecurity awareness and digital banking adoption: Exploring the moderating impact of digital literacy. *International Journal of Economics and Finance Studies*, *16*(3), 34-58. https://doi.org/10.34109/ijefs.202416303
2. Alrababah, H., Iqbal, H., Khan, M.A. (2024). The effect of user behavior in online banking on cybersecurity knowledge. *International Journal of Intelligent Systems*, *1,* 9949510. https://doi.org/10.1155/int/9949510
3. Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 2693080. https://doi.org/10.1155/2022/2693080
4. Cele, N.N., Kwenda, S. (2023). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *30*(8), 104-122. https://doi.org/10.1108/JFC-10-2023-0263
5. CERT Polska (2024). *Raport o stanie bezpieczeństwa w polskim internecie 2024*. NASK. https://cert.pl/raport2024
6. Chen, S., Doerr, S., Frost, J., Gambacorta, L., Shin, H.S. (2023). The fintech gender gap. *Journal of Financial Intermediation*, *54*, 101026. https://doi.org/10.1016/j.jfi.2023.101026
7. Chicco, D., Sichenze, A., Jurman, G. (2025). A simple guide to the use of Student's t-test, Mann-Whitney U test, Chi-squared test, and Kruskal-Wallis test in biostatistics. *BioData Mining*, *18*, 56. https://doi.org/10.1186/s13040-025-00465-6
8. Coopamootoo, K.P., Ng, M. (2023). *Un-Equal Online Safety? A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns*. Proceedings of the 32nd USENIX Security Symposium (USENIX Security '23) (pp. 5611-5628). USENIX Association.
9. Enock, F.E., Stevens, F., Bright, J., Cross, M., Johansson, P., Wajcman, J., Margetts, H.Z. (2024). Understanding gender differences in experiences and concerns surrounding online harms: A short report on a nationally representative survey of UK adults. *arXiv.* https://doi.org/10.48550/arXiv.2402.00463
10. European Union Agency for Cybersecurity (ENISA) (2024). *Threat Landscape 2024: Trends and Threats in the European Union*. ENISA Publications.
11. Hossain, M.A. (2019). Security perception in the adoption of mobile payment and the moderating effect of gender. *PSU Research Review*, *3*(3), 179-190. https://doi.org/10.1108/PRR-03-2019-0006
12. International Telecommunication Union (ITU) (2023). *Global Cybersecurity Index 2023*. Geneva: ITU Publications.

13. Kuzior, A., Tiutiunyk, I., Zielińska, A., Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies*, *17*(2), 220-239. https://doi.org/10.14254/2071-8330.2024/17-2/12
14. Liu, F., Lyons, A.C., Fang, E.S. (2025). Risk, gender, and digital finance. *Finance Research Letters*, *79*, 107295. https://doi.org/10.1016/j.frl.2025.107295
15. Lobão, J. (2024). The Influence of Gender on Individuals' Ability to Predict Their Own Risk Tolerance: Evidence from a European Country. *Administrative Sciences*, *14*(3), 56. https://doi.org/10.3390/admsci14030056
16. McGill, T., Thompson, N. (2018). *Gender differences in information security perceptions and behaviour.* Proceedings of the 29th Australasian Conference on Information Systems (ACIS 2018).
17. Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia – Social and Behavioral Sciences*, *147*, 424-428. https://doi.org/10.1016/j.sbspro.2014.07.133
18. Mroczko, J.A., Bręborowicz, G.H., Tadeusiewicz, R. (1998). *Statystyka w badaniach medycznych*. PWN.
19. Murphy, G.B., Tocher, N. (2011). Gender differences in the effectiveness of online trust building information cues: An empirical examination. *The Journal of High Technology Management Research*, *22*(1), 26-35. https://doi.org/10.1016/j.hitech.2011.03.004
20. Prajzner, A. (2022). Wybrane wskaźniki wielkości efektu w badaniach psychologicznych. *Annales Universitatis Mariae Curie-Skłodowska. Sectio J. Paedagogia-Psychologia*, *35*(4), 139-157. https://doi.org/10.17951/j.2022.35.4.139-157
21. Sholevar, M., Bachmann, R. (2025). Patterns of trust in financial services: critical factors and gender differences. *Journal of Financial Services Marketing*, *30*, 1-15. https://doi.org/10.1057/s41264-025-00303-0
22. Sikakebieke, M., Kuanova, L. (2025). Gender Gap in Digital Banking Usage in Emerging Markets: Evidence from Kazakhstan's Digital Transformation. *Eurasian Journal of Gender Studies*, *2*(2), 28-39. https://doi.org/10.47703/ejgs.v2i2.38
23. Sulaiman, N.S., Fauzi, M.A., Hussain, S., Wider, W. (2022). Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyberattacks. *Information*, *13*(9), 413. https://doi.org/10.3390/info13090413
24. Warszawski Instytut Bankowości (2024). *Raport Cyberbezpieczny portfel (Edycja V).* https://cyber.wib.edu.pl/wp-content/uploads/2025/10/raport_Cyberbezpieczny-portfel-2024.pdf
25. Warszawski Instytut Bankowości (2025). *Postawy Polaków wobec cyberbezpieczeństwa (Edycja VI)*. https://cyber.wib.edu.pl/wp-content/uploads/2025/10/fragment-badania-Postawy-Polakow-wobec-cyberbezp._VII-2024.pdf

26. Wiktorowicz, J., Grzelak, M.M., Grzeszkiewicz-Radulska, K. (2020). *Analiza statystyczna z IBM SPSS Statistics*. Wydawnictwo Uniwersytetu Łódzkiego. https://doi.org/10.18778/8220-387-5
27. Yadav, P., Kumar, A., Mishra, S.K., Kochhar, K. (2024). Financial equality through technology: Do perceived risks deter Indian women from sustained use of mobile payment services? *International Journal of Information Management Data Insights*, *4*, 100266. https://doi.org/10.1016/j.jjimei.2024.100266