risks

MDPI

Article

Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy

Alexandru Răzvan Căciulescu [1], Răzvan Rughiniș [1,2,*], Dinu Țurcanu [3] and Alexandru Radovici [1]

[1] Faculty of Automatic Control and Computers, National University of Science and Technology Politehnica Bucharest, 060042 Bucharest, Romania; acaciulescu@upb.ro (A.R.C.); alexandru.radovici@upb.ro (A.R.)
[2] Academy of Romanian Scientists, 3 Ilfov, 050044 Bucharest, Romania
[3] Faculty of Electronics and Telecommunications, National Institute of Innovations in Cybersecurity "CYBERCOR", Technical University of Moldova, MD-2004 Chișinău, Moldova; dinu.turcanu@adm.utm.md
* Correspondence: razvan.rughinis@upb.ro; Tel.: +40-722-302-269

Abstract: This study investigates the landscape of cyber-financial risks across Europe by identifying distinct risk profiles based on financial literacy, digital comfort, and economic vulnerability. Utilizing data from the Flash Eurobarometer 525 survey, we employ K-means cluster analysis to categorize European citizens into five distinct cyber-financial risk profiles: Cyber-Savvy Pragmatists, Digital-Savvy Vulnerable individuals, Cautious Traditionalists, Comfortably Naive individuals, and Digitally Hesitant At-Risk individuals. Our findings show significant variations in risk profiles across demographic groups and European regions, with gender disparities and educational differences. We examine how self-perceived financial knowledge and financial decision-making patterns differ across these profiles, uncovering potential overconfidence in some groups that may exacerbate cyber-financial vulnerabilities. This study also explores regional distributions of risk profiles, highlighting areas of heightened cybersecurity concern across Europe. Our results indicate that cybersecurity strategies should be tailored to address the specific vulnerabilities of each risk profile, with particular attention to gender-based disparities and regional variations. This research contributes to a better understanding of cyber-financial risks in Europe and offers actionable information for policymakers, financial institutions, and cybersecurity professionals in developing targeted interventions to enhance digital financial security across diverse populations.

Keywords: cyber-financial risks; financial literacy; cybersecurity; digital finance; European Union; cluster analysis

Citation: Căciulescu, Alexandru Răzvan, Răzvan Rughiniș, Dinu Țurcanu, and Alexandru Radovici. 2024. Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. *Risks* 12: 200. https://doi.org/10.3390/risks12120200

Academic Editor: Roy Cerqueti

Received: 28 October 2024
Revised: 25 November 2024
Accepted: 3 December 2024
Published: 10 December 2024

1. Introduction

In today's digital age, the intersection of financial literacy and cybersecurity has become increasingly important. As more people rely on online platforms for banking, investing, and managing their finances, the risks associated with poor financial knowledge and digital insecurity grow. Financially vulnerable individuals, those unfamiliar with digital financial services, or those lacking in financial education may be more susceptible to online fraud, phishing attacks, and investment scams. A recent Eurobarometer study on financial literacy in the EU highlights not only the gaps in people's understanding of financial concepts but also their comfort with using digital tools. These gaps present significant cybersecurity risks, as individuals who struggle with financial literacy may also be less equipped to recognize and avoid cyber threats.

The increasing importance of cybersecurity in daily life is driven by several converging factors. The rapid digitalization of essential services, particularly financial transactions, has moved traditionally offline activities into the digital realm. The COVID-19 pandemic accelerated this shift, making digital financial services not just a convenience but a necessity for many. Simultaneously, cybercriminals have become more sophisticated, employing advanced technologies and social engineering techniques to exploit vulnerabilities. The

rise of mobile banking, contactless payments, and cryptocurrency markets has created new attack vectors. Moreover, the interconnected nature of modern financial systems means that security breaches can have cascading effects, impacting entire economic networks. This heightened risk landscape raises the social and scientific priority for understanding and addressing cyber-financial vulnerabilities.

The relationship between cybersecurity and cyber finance is mutually reinforcing. Cybersecurity serves as the protective framework that enables the safe operation of digital financial services, while the evolution of cyber finance continuously shapes cybersecurity requirements and challenges. This relationship manifests itself in several ways: First, cybersecurity measures protect the integrity of financial transactions, safeguarding against unauthorized access and fraud while maintaining the confidentiality of sensitive financial data. Second, the rapid innovation in financial technologies (such as mobile banking, digital wallets, and cryptocurrency) necessitates continuous advancement in cybersecurity protocols to address emerging threats. Third, cybersecurity failures in financial systems can have immediate monetary consequences, making the financial sector a prime target for cybercriminals and thereby demanding more robust security measures. Fourth, regulatory compliance in cyber finance often drives cybersecurity standards, as financial institutions must meet strict security requirements to protect customer assets and data. Understanding this relationship is highly important, as vulnerabilities in either domain can cascade into the other, potentially compromising both financial assets and personal information.

The Flash Eurobarometer 525 "Monitoring the level of financial literacy in the EU" Report (European Commission 2023a) highlights several potential risks that various demographic groups face when engaging with financial matters online, stemming from gaps in financial literacy, financial vulnerability, and varying comfort levels with digital financial services. The report indicates significant disparities in financial literacy across EU member states and demographic groups. On average, only 18% of EU respondents demonstrated high overall financial literacy, with scores varying widely between countries. Notably, certain groups consistently showed lower financial literacy, including women, younger individuals (aged 18–24), those with lower education levels, and manual workers. This gap in financial knowledge and skills may leave these groups more susceptible to poor financial decision making and potential exploitation in digital financial environments.

Financial vulnerability is another key risk factor identified in the report. Approximately 16% of EU respondents reported having no emergency savings, with this figure rising to over 20% in several countries. Again, those with lower education levels, manual workers, and non-working individuals were more likely to lack financial buffers. This vulnerability could lead to increased susceptibility to high-risk financial products or predatory lending practices encountered online.

Comfort with digital financial services also varied significantly. While 77% of EU respondents reported feeling comfortable using such services, there were notable differences across countries and demographic groups. Older individuals (aged 55+), those with lower education levels, and manual workers expressed less comfort with digital financial tools. This discomfort could potentially lead to exclusion from beneficial digital financial services or increased vulnerability to fraud when forced to use unfamiliar digital platforms.

The combination of low financial literacy, financial vulnerability, and discomfort with digital services creates a particularly high-risk profile. Individuals falling into multiple at-risk categories may struggle to critically evaluate online financial information, lack the financial resilience to withstand poor decisions, and feel pressured or confused when navigating digital financial interfaces. This could lead to a range of negative outcomes, from falling victim to online scams to making ill-informed investment decisions or accumulating unsustainable debt through easily accessible digital credit products.

Moreover, the report indicates generally low confidence in investment advice received from financial institutions, with only 38% of EU respondents expressing confidence that such advice prioritizes their best interests. This lack of trust, combined with low financial

literacy, could drive individuals towards unregulated or high-risk investment opportunities encountered online.

Building upon the existing literature, this study aims to address several questions regarding cyber-financial risks in Europe. Specifically, we seek to identify distinct cyber-financial risk profiles among European citizens based on their configurations of financial knowledge, financial vulnerability, and comfort with digital financial services. We then explore how self-perceived financial knowledge levels vary across these profiles and examine patterns of financial decision making within each group. Furthermore, we investigate how socio-demographic factors such as gender, age, and education level correlate with the identified risk profiles. Finally, we analyze regional variations in the distribution of these profiles across European countries. By addressing these questions, we aim to increase the understanding of the cyber-financial risk landscape in Europe, identifying vulnerable groups and the factors contributing to their susceptibility to cyber threats in the digital financial ecosystem.

The remainder of this paper is structured as follows: First, we synthesize the state of the art. We then discuss our data and methods, detailing the Flash Eurobarometer 525 survey data and the K-means cluster analysis technique employed to identify cyber-financial risk profiles. Next, we present our results, beginning with a detailed description of the five identified risk clusters. We then analyze variations in self-perceived financial knowledge and financial decision-making patterns across these clusters. This is followed by an examination of socio-economic characteristics and regional distributions of the risk profiles. In the discussion section, we interpret our findings in the context of existing literature and explore their implications for cybersecurity in Europe. We also address the limitations of our study and suggest directions for future research. Finally, we conclude with policy recommendations aimed at enhancing cyber-financial resilience across different segments of the European population.

2. State of the Art

There is a substantial body of scientific research investigating the intersection of financial literacy and cybersecurity. Cyber-financial risks and vulnerabilities are primarily defined as threats to individuals' financial security and personal information in digital environments. These risks encompass a range of malicious activities that exploit technological and human vulnerabilities to gain unauthorized access to financial resources or sensitive data.

2.1. Types and Nature of Cyber-Financial Risks

The main types of cyber-financial attacks discussed in the literature include phishing, identity theft, online fraud, and unauthorized access to financial accounts. Phishing, a prevalent form of attack, involves deceptive attempts to acquire sensitive information by masquerading as trustworthy entities (Abroshan et al. 2021; Broadhurst et al. 2019). This can occur through various channels, with email being a common vector (Rey-Ares et al. 2024). Recent research by Ribeiro et al. (2024) further identifies key factors affecting phishing susceptibility, such as detection self-efficacy, internet activities related to services, and prior experiences with cyber-victimization. Identity theft, another significant cyber-financial risk, is defined as the unlawful use of personal or financial information obtained online without the owner's consent (Guedes et al. 2023). This type of attack can lead to financial losses and reputational damage for the victims. Online fraud, particularly in the context of e-commerce and online banking, is also highlighted as a major concern (Houtti et al. 2024). Unauthorized access to financial accounts, including the use of stolen credit card information or hacking of bank accounts, represents another key cyber-financial risk (Abdulai 2020). This can result in direct financial losses for victims and undermines trust in digital financial systems. Several studies also emphasize the role of social engineering in these attacks (Hossain et al. 2024), where cybercriminals exploit psychological vulnerabilities to manipulate individuals

into divulging sensitive information or performing actions that compromise their financial security (Whitty 2019; Judges 2021).

2.2. Digital Financial Services and Emerging Risks

The literature also recognizes emerging risks associated with the increasing digitalization of financial services (Mishra 2023; Al-Kumaim and Alshamsi 2023). For instance, Koskelainen et al. (2023) highlight the challenges posed by Fintech innovations, such as mobile banking and digital payments, which create new avenues for cyber-financial attacks. In the context of organizational cybersecurity, particularly in the banking sector, cyber-financial risks are viewed as threats to both the institutions and their customers. These include various forms of fraud, hacking, and malware attacks targeting financial institutions and their digital infrastructure (Isa et al. 2021). Ahmed et al. (2024) investigate the factors influencing customer protection in Pakistan's digital banking sector, finding that information security, responsiveness, data privacy, authentication mechanisms, and encryption all positively impact customer protection, with information security being the most significant factor.

2.3. Financial Literacy and Cybersecurity

Individuals' financial literacy plays a dual role in both creating and mitigating cyber-financial risks, as evidenced by several studies in the reviewed literature, with some aspects of financial literacy serving as protective factors, while others potentially increasing exposure to risks. Rey-Ares et al. (2024) found that both objective and subjective financial knowledge increased the likelihood of exposure to fraudulent emails, contradicting the hypothesis that knowledge protects against fraud. This suggests that individuals with higher financial literacy may engage more frequently with financial products and online platforms, inadvertently increasing their exposure to cybercriminals. However, the same study also found that objective financial knowledge reduces the likelihood of becoming a victim after exposure, indicating that financially knowledgeable individuals are better equipped to detect scams and avoid falling for fraudulent schemes. The importance of financial literacy in combating cybercrime is particularly emphasized in the banking sector. Isa et al. (2021) found that employees with better financial knowledge are more adept at recognizing phishing attempts and other forms of cybercrime, making them less likely to fall victim to such attacks. Kovács and Terták (2024) also argue that financial literacy is the best defense against cybercrime. They posit that individuals who are aware of how cyberattacks work, particularly phishing, ransomware, and identity theft, are less likely to fall victim. Their study emphasizes that financial literacy must include knowledge of digital security practices such as safe internet use, password protection, and recognizing phishing schemes. Recent research by Amnas et al. (2024) highlights the positive impact of FinTech on financial inclusion, emphasizing the crucial mediating role of digital financial literacy and the moderating effect of perceived regulatory support, which aligns with our study's focus on the intersection of financial knowledge and digital comfort in shaping cyber-financial risk profiles.

However, the relationship between financial literacy and cyber-financial risks is not always straightforward. Judges (2021) found that cognitive factors, such as processing speed and working memory, play a significant role in scam susceptibility among older adults. This suggests that while financial literacy is important, cognitive abilities also play a crucial role in protecting against cyber-financial risks. Whitty (2019) introduces an interesting observation by highlighting the role of financial overconfidence. The study found that while objective financial knowledge can protect against victimization, subjective financial knowledge and overconfidence can increase the risk of falling victim to scams.

2.4. Cognitive Factors in Cyber-Financial Security

The relationship between memory and cyber-financial security emerges as a critical factor in understanding vulnerability to cyber threats. Memory affects multiple aspects

of cyber-financial security (Judges 2021): the ability to remember complex passwords without resorting to unsafe storage practices, the capacity to recognize patterns in previous suspicious interactions, and the facility to maintain awareness of multiple security concerns while conducting financial transactions. Memory demands in cybersecurity can be particularly challenging for older adults, as noted by Whitty (2019), who may struggle with remembering multiple passwords or security protocols across different financial platforms. Moreover, the increasing complexity of digital financial services places greater demands on working memory, requiring users to simultaneously process security warnings, transaction details, and authentication steps. This cognitive load can lead to security fatigue, where users may choose convenience over security, potentially compromising their financial safety.

Koskelainen et al. (2023) emphasize the need for a revised financial literacy framework that incorporates digital financial literacy. Their study shows that traditional financial literacy alone is insufficient in the digital world, and consumers must develop new skills to understand and mitigate risks associated with digital financial tools and services.

2.5. Socio-Economic and Psychological Factors

The literature reviewed highlights several factors beyond financial literacy that influence cyber-financial risks and vulnerabilities. Financial vulnerability is a significant consideration. Houtti et al. (2024) found that countries with lower Gross National Income (GNI) per capita are more vulnerable to scams, with a strong inverse correlation between GNI per capita and scam victimization. Thus, economic hardship may increase susceptibility to cyber-financial risks, possibly due to individuals being more likely to engage with risky financial opportunities out of necessity or desperation.

Comfort with and frequency of using digital financial apps and platforms play a dual role in cyber-financial risks. Lee and Kim (2020) found that individuals who frequently engaged in service-related activities, such as online banking or accessing state services, were more susceptible to phishing. However, their study also indicated that those with higher technological competencies were better equipped to protect themselves against cyber threats. At the national level, the degree of cybersecurity awareness and preparedness is another important factor. Lee and Kim (2020) found that countries with stronger cybersecurity infrastructures, as measured by the Global Cybersecurity Index, tend to have citizens with better individual preparedness against cyber threats.

Social isolation and loneliness have been identified as significant contributors to cyber-financial victimization, particularly among older adults. Judges (2021) found that older adults experiencing more socioemotional disturbance due to social isolation are at a higher risk of fraud victimization. Other psychological factors, particularly risk-taking behavior and decision-making styles, also play a role in cyber-financial vulnerabilities. Abroshan et al. (2021) found that general risk-taking behavior significantly predicts the likelihood of clicking on phishing links. However, their study also noted that decision-making styles (e.g., rational and intuitive) did not significantly affect phishing susceptibility. Cultural and geographical factors also shape cyber-financial risks. Broadhurst et al. (2019) found that international students were more susceptible to phishing attacks than domestic students, possibly due to language barriers and unfamiliarity with local systems.

Individuals may construct different realities around financial technologies and cybersecurity, shaping their risk profiles and behaviors in digital financial environments. The construction of divergent worldviews in scientific matters, as explored by Rughiniş and Flaherty (2022), also influences how individuals with different levels of financial literacy and digital comfort perceive and respond to cyber-financial risks. Similarly, the emerging social status of generative AI as a social actor, with dual interpretations of competence or incompetence (Bran et al. 2023), highlights how public discourse shapes divergent perceptions of technological competence and risk.

Lastly, the psychological impact of past victimization plays a role in shaping future vulnerability to cyber-financial risks. Abdulai (2020) found that individuals who have been

victims of cybercrime are more likely to fear future victimization, which can influence their online behavior and potentially their vulnerability to future attacks.

2.6. Demographic Patterns in Cyber-Financial Risks

Socio-demographic differences in gender, age, and education levels also play significant roles in shaping cyber-financial risks and vulnerabilities, although their effects are not always consistent across studies and can vary depending on the specific type of cyber-financial risk being examined. Gender differences in cyber-financial risks have been observed in several studies, though the findings are not always consistent. Abroshan et al. (2021) found that women were more likely to click on phishing links than men, suggesting a potential gender-based vulnerability in this specific aspect of cyber-financial risk. Similarly, Guedes et al. (2023) initially found that women reported higher levels of fear of online identity theft, although this difference diminished when other variables were considered in multivariate models. However, Wei et al. (2024) noted that gender differences in security behavior are mixed, with women generally more focused on privacy, while men are more engaged in technical security practices.

Different age groups show specific vulnerabilities to different types of risks. Sheng et al. (2010) found that participants between 18 and 25 years old were more likely to fall for phishing than other age groups, attributing this to lower levels of education, fewer years of internet experience, and less aversion to financial risk among younger participants. Conversely, Judges (2021) and Whitty (2019) identified older adults as being more vulnerable to certain types of cyber-fraud, particularly due to cognitive decline and lower digital literacy. Koskelainen et al. (2023) noted that while younger individuals are more familiar with digital financial tools, they may be prone to impulsive behavior, whereas older individuals may struggle with the complexity of digital services.

Education levels generally correlate with lower cyber-financial risks, although the relationship is not always straightforward. Isa et al. (2021) found that higher education levels, particularly postgraduate degrees, were associated with better awareness and preventive measures against cybercrime in the banking sector. Similarly, Wei et al. (2024) noted that higher education is associated with a greater likelihood of using advanced security measures like two-factor authentication. However, Rey-Ares et al. (2024) found that higher education levels were correlated with increased fear and perceived risk of online identity theft, possibly due to greater awareness of cyber threats.

The intersection of these demographic factors can create specific risk profiles. For instance, Judges (2021) found that older women may be more susceptible to specific types of fraud, highlighting the importance of considering multiple demographic factors in understanding cyber-financial vulnerabilities. Additionally, Broadhurst et al. (2019) identified international students and first-year students as being significantly more likely to fall for phishing scams than domestic and later-year students, suggesting that factors such as language barriers and unfamiliarity with local systems can compound age-related vulnerabilities.

It is important to note that the effects of gender, age, and education on cyber-financial risks can be mediated by other factors such as financial literacy, digital competence, and cybersecurity awareness. For example, Lee and Kim (2020) found that individuals with higher education levels may have better access to scam-related knowledge but may still fall victim due to cognitive aging or overconfidence.

2.7. Research Gaps

Despite the extensive research on cyber-financial risks, several important gaps remain in the current literature. First, while existing studies have examined individual factors like financial literacy, digital comfort, or economic vulnerability separately, there has been limited investigation into how these factors interact to create distinct risk profiles within populations. Second, although previous research has identified demographic variations in cyber-financial risks, few studies have mapped these variations across the entire European Union, leaving a gap in our understanding of regional patterns and disparities. Third,

the relationship between self-perceived and actual financial knowledge, particularly in the context of digital financial services, has not been thoroughly explored across different population segments. Our study addresses these gaps by employing cluster analysis to identify distinct cyber-financial risk profiles, examining their distribution across European regions, and analyzing the alignment between perceived and actual financial knowledge within these profiles.

3. Data and Methods

This research employs a secondary data analysis approach, utilizing data from the Flash Eurobarometer 525 survey conducted between March and April 2023 "Monitoring the level of financial literacy in the EU" (European Commission 2023a). This Eurobarometer survey provides a comprehensive dataset on financial literacy, digital financial services usage, and socio-economic characteristics across the European Union member states. Data were weighted to be representative of the EU27 population. We conducted statistical analyses using the IBM SPSS software version 29.0.2.0 and visualizations with Excel from Microsoft Office 365.

This study employed a three-phase methodological approach to analyze cyber-financial risk patterns across the European Union. The first phase involved an overview analysis of the Flash Eurobarometer 525 dataset, which provided granular information on citizens' financial literacy, digital service engagement, and economic vulnerability. In the second phase, we applied K-means cluster analysis to identify distinct cyber-financial risk profiles, optimizing for both within-cluster homogeneity and between-cluster separation. This clustering approach enabled the identification of patterns in how financial knowledge, digital comfort, and economic vulnerability intersect across populations. This classification technique allows for the identification of relatively homogeneous groups within the data based on selected variables. The final phase consisted of detailed profiling of the identified clusters through demographic and regional analyses, examining how these risk profiles manifest across different socio-economic strata and geographical contexts. The following sections detail the specific analytical procedures and statistical considerations employed in each phase.

In our analysis, we focused on three key dimensions: financial knowledge, financial vulnerability, and comfort with digital financial services. Financial knowledge was measured by the number of correct responses to five financial knowledge questions in the survey, namely, Q2, Q3, Q4, Q5, and Q6, as follows (European Commission 2023b):

Q2: Imagine that someone puts EUR 100 into a savings account with a guaranteed interest rate of 2% per year. They don't make any further payments into this account, and they don't withdraw any money. How much would be in the account at the end of five years, once the interest payment is made? 1 = "More than EUR 110"; 2 = "Exactly EUR 110"; 3 = "Less than EUR 110"; 4 = "Don't know".

Q3: Now imagine the following situation. You are going to be given a gift of [EUR 1000] in one year and, over that year, inflation stays at 2%. In one year's time, with the [EUR 1000], will you be able to buy 1 = "More than you could buy today"; 2 = "The same amount"; 3 = "Less than you could buy today"; 4 = "Don't know".

Q4: If interest rates rise, what will typically happen to bond prices? 1 = "They will rise"; 2 = "They will fall"; 3 = "They will stay the same, as there is no relationship between bond prices and the interest rate"; 4 = "Don't know".

Q5: Which of the following is true? An investment with a higher return is likely to be 1 = "More risky than an investment with a lower return"; 2 = "Less risky than an investment with a lower return"; 3 = "As risky as an investment with a lower return"; 4 = "Don't know".

Q6: An investment in a wide range of "company shares" is likely to be 1 = "More risky than an investment in a single share"; 2 = "Less risky than an investment in a single share"; 3 = "As risky as an investment in a single share"; 4 = "Don't know".

Financial vulnerability was assessed through the question, "If you lost your main source of income today, how long could you continue to cover your living expenses, without borrowing any money or moving house?" Comfort with digital financial services was evaluated based on responses to the question, "How comfortable are you with using digital financial services, such as online banking or mobile payments?" Descriptive values for indicators used in the analysis are presented in Table 1.

Table 1. Descriptive statistics for key variables used in cyber-financial risk analysis. This table presents the sample size (N), minimum, maximum, mean values, and standard deviations for variables measuring financial knowledge (based on responses to five knowledge questions); financial vulnerability (ability to cover expenses after income loss); comfort with digital financial services; self-perceived financial knowledge; and demographic characteristics including gender, age, and education level. Data source: Flash Eurobarometer 525 survey, 2023.

Variables	N	Minimum	Maximum	Mean	Std. Deviation
Financial knowledge score—number of correct responses to the five financial knowledge questions (Q2, Q3, Q4, Q5, and Q6)	26,125	0	5	2.52	1.32
Q8: If you lost your main source of income today, how long could you continue to cover your living expenses, without borrowing any money or moving house? 1 = "I don't have emergency savings"; 2 = "At least 1 week, but less than 1 month"; 3 = "At least 1 month, but not 3 months"; 4 = "At least 3 months, but not 6 months"; 5 = "6 months or more"	24,013	1	5	3.48	1.49
Q11: How comfortable are you with using digital financial services, such as online banking or mobile payments? 4 = "Very comfortable"; 3 = "Somewhat comfortable"; 2 = "Not too comfortable"; 1 = "Not at all comfortable"	25,672	1	4	3.08	0.88
Self-perceived knowledge: How would you rate your overall knowledge about financial matters compared to other adults in [COUNTRY]? 1 = "Very low"; 2 = "Quite low"; 3 = "About average"; "4 = "Quite high"; 5 = "Very high"	25,786	1	5	3.17	0.85
Gender 0 = "Male"; 1 = "Female"	26,071	0	1	0.52	0.50
Age exact (years)	26,125	18	97	49.53	16.83
ISCED Level of education: 1 = "Low education"; 2 = "Medium education"; 3 = "High education"	26,125	1	3	2.11	0.71
Valid N (listwise)	23,464				

In our analysis, we opted for a 5-cluster solution. This decision was made to obtain a nuanced classification that is still interpretable, supported by a comparative analysis of within-to-between cluster variance ratios across solutions with three to six clusters (see Supplementary Materials). The 5-cluster solution provides optimal separation across all variables, particularly for digital service usage patterns, while maintaining analytical parsimony. At the same time, five clusters remain manageable for analyses and practical applications, with each cluster representing a distinct and meaningful profile that can inform targeted interventions and policies (Vulpe and Rughiniș 2021; Rughiniș et al. 2022). The resulting clusters were then profiled using various socio-demographic variables such as age, gender, education level, and country of residence.

4. Results

4.1. Cluster Analysis

The analysis of cyber-financial risk profiles showed specific vulnerabilities and strengths across five distinct clusters, each facing specific challenges in the digital financial ecosystem. These clusters, identified through K-means analysis, classify the interactions between financial knowledge, economic vulnerability, and digital comfort that shape individuals' susceptibility to cyber-financial risks (see Table 2 and Figure 1).

Table 2. Characteristics of the five identified cyber-financial risk profiles. This table presents mean scores for each cluster on three key dimensions: financial knowledge (number of correct responses to five financial literacy questions, range 0–5); financial vulnerability (ability to cover expenses after income loss, range 1–5, where 1 = no emergency savings and 5 = 6+ months coverage); and comfort with digital financial services (range 1–4, where 1 = not at all comfortable and 4 = very comfortable). The relative size of each cluster is shown as both count (N) and percentage of the total sample. Data source: Flash Eurobarometer 525 survey, 2023.

	1	2	3	4	5
	Cyber-Savvy Pragmatists	**Digital-Savvy Vulnerable Individuals**	**Cautious Traditionalists**	**Comfortably Naive Individuals**	**Digitally Hesitant At-Risk Individuals**
Financial knowledge score: number of correct responses to the five financial knowledge questions in the survey (Q2, Q3, Q4, Q5, and Q6)	3.82	3.51	2.60	1.42	1.13
Financial vulnerability: "If you lost your main source of income today, how long could you continue to cover your living expenses, without borrowing any money or moving house?" [Values: 1 = "I don't have emergency savings"; 2 = "At least 1 week, but less than 1 month"; 3 = "At least 1 month, but not 3 months"; 4 = "At least 3 months, but not 6 months"; 5 = "6 months or more"]	4.78	1.91	3.78	4.39	1.59
Comfortable with digital financial services: "How comfortable are you with using digital financial services, such as online banking or mobile payments?" [Values: 4 = "Very comfortable"; 3 = "Somewhat comfortable"; 2 = "Not too comfortable"; 1 = "Not at all comfortable"]	3.49	3.28	2.16	3.39	2.83
Cluster membership (N)	7175	3800	4330	5336	5484
Cluster membership (%)	27%	15%	17%	20%	21%

Cyber-Savvy Pragmatists, with their high scores across all dimensions (financial knowledge, 3.82; stability, 4.78; and digital comfort, 3.49), are best positioned to navigate cyber-financial risks. However, they are not immune. Their confidence might make them targets for highly sophisticated phishing attempts or advanced persistent threats (APTs) targeting high-value individuals. They may also face risks related to over-optimization, where their knowledge leads them to complex financial products or strategies that, while potentially beneficial, increase their exposure to market volatility or systemic risks in the digital finance ecosystem.

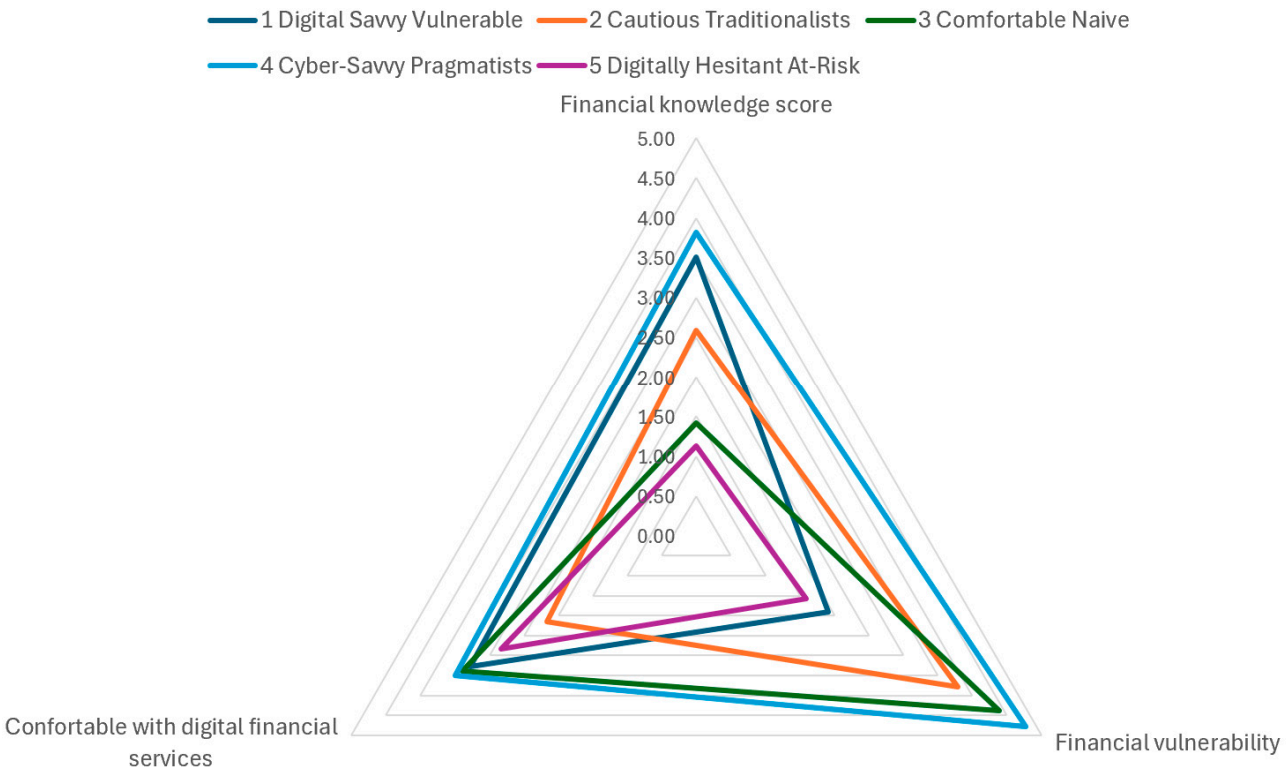


Figure 1. Radar plot comparing the five cyber-financial risk profiles across three key dimensions: financial knowledge (scale 0–5, based on correct responses to knowledge questions); financial vulnerability (scale 1–5, measuring ability to cover expenses after income loss); and digital comfort (scale 1–4, measuring comfort with digital financial services). Each profile represents a distinct combination of these characteristics, illustrating the varied nature of cyber-financial risks across the European population. Data source: Flash Eurobarometer 525 survey, 2023.

The Digital-Savvy Vulnerable cluster presents an intriguing paradox. With moderate financial knowledge (3.51) and high digital comfort (3.28), this group navigates online financial services with ease. However, their high financial vulnerability (1.91) exposes them to significant risks. They may be prone to phishing attacks that exploit their familiarity with digital platforms or fall victim to investment scams that promise quick solutions to their financial instability. Their comfort with technology, combined with financial pressure, could lead them to overextend themselves through easily accessible digital credit services.

Cautious Traditionalists, characterized by low-moderate financial knowledge (2.60) and low digital comfort (2.16), face a different set of challenges. Their moderate financial stability (3.78) provides some buffer, but their limited engagement with digital financial services may leave them vulnerable to offline financial fraud or miss out on the security features of modern banking systems. When they do venture online, their unfamiliarity might make them susceptible to basic cyber threats or social engineering tactics that more digitally savvy individuals might easily recognize.

The Comfortably Naive cluster presents a unique risk profile. Despite high financial stability (4.39) and digital comfort (3.39), their very low financial knowledge (1.42) makes them prime targets for sophisticated investment scams. Their comfort with digital platforms, coupled with a lack of financial acumen, could lead them to fall for high-yield investment programs (HYIPs) or cryptocurrency scams that promise unrealistic returns. They may also be vulnerable to identity theft due to an oversharing of financial information online, not fully understanding the implications of their digital footprint.

The Digitally Hesitant At-Risk cluster faces perhaps the most severe cyber-financial risk profile. With very low financial knowledge (1.13), high financial vulnerability (1.59), and moderate digital comfort (2.83), they are susceptible to a wide range of threats. Their

financial pressure may make them targets for predatory lending schemes, both online and offline. Their moderate digital comfort suggests they use online financial services, but likely without fully understanding the associated risks, making them vulnerable to man-in-the-middle attacks, credential stuffing, or other technical exploits. Their low financial knowledge may also lead them to make poor decisions when faced with financial products or services they do not fully understand, whether encountered online or in traditional settings.

4.2. Self-Perceived Financial Knowledge Across Clusters

We examined variations in self-assessed financial knowledge across cyber-financial risk profiles, using answers to the following question: How would you rate your overall knowledge about financial matters compared to other adults in [COUNTRY]? 1 = "Very low"; 2 = "Quite low"; 3 = "About average"; 4 = "Quite high"; 5 = "Very high". Across all clusters, the majority of individuals rate their financial knowledge as "about average", with percentages ranging from 49% to 58% (see Figure 2). This clustering around the average could reflect a general tendency towards modest self-assessment or a lack of clear benchmarks for what constitutes high or low financial knowledge.

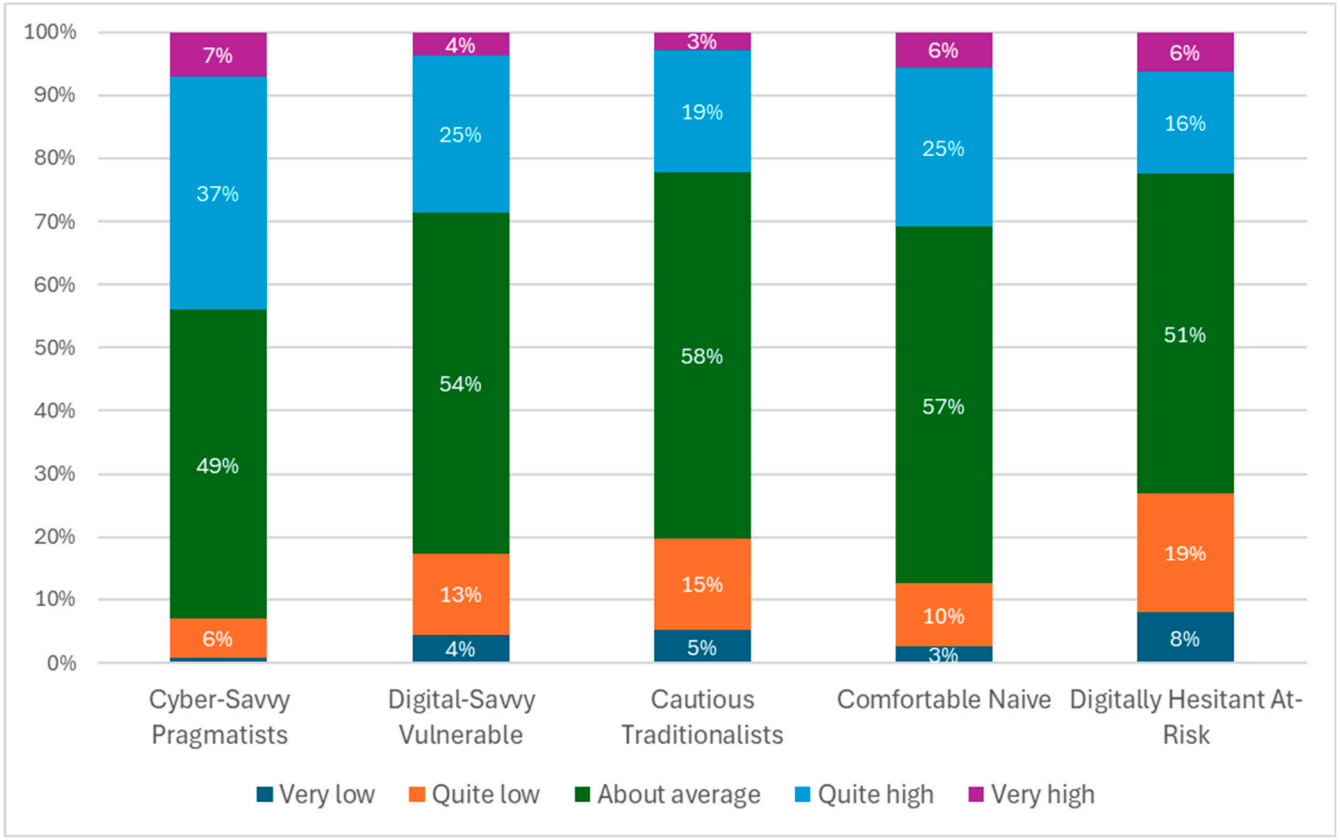


Figure 2. Distribution of self-perceived financial knowledge across the five cyber-financial risk profiles. This graph shows the percentage of individuals within each cluster who rate their financial knowledge as very low, quite low, about average, quite high, or very high compared to other adults in their country. This distribution reveals potential mismatches between perceived and actual financial knowledge across different risk profiles. Data source: Flash Eurobarometer 525 survey, 2023.

The presence of individuals who rate their knowledge as "very high" across all clusters, including those characterized by lower objective financial literacy, is noteworthy. This could indicate a persistent overconfidence bias in a small subset of each population, regardless of actual financial acumen.

Cyber-Savvy Pragmatists demonstrate the highest level of confidence in their financial knowledge, with 44% rating their knowledge as quite high or very high. This aligns well with their cluster characteristics, suggesting a good match between perceived and actual financial literacy. However, it is noteworthy that nearly half (49%) of this group still considers their knowledge "about average", which could indicate a degree of modesty or realistic self-assessments among even the most financially literate group.

The Digital-Savvy Vulnerable cluster presents an interesting case. Despite their digital savviness, only 29% rate their financial knowledge as quite high or very high, with the majority (54%) considering it average. This self-assessment appears to align with their cluster profile, suggesting a realistic understanding of their financial vulnerabilities despite their comfort with digital tools.

Cautious Traditionalists show the lowest levels of high self-perceived financial knowledge, with only 22% rating themselves as quite high or very high. This conservative self-assessment matches their cautious approach to financial matters and digital services, indicating a potential lack of confidence that may contribute to their hesitancy in engaging with modern financial tools.

The Comfortably Naive cluster presents a particularly intriguing pattern. Despite being characterized by low objective financial knowledge, 31% of the Comfortably Naive group rates their financial knowledge as quite high or very high—a higher proportion than both the Digital-Savvy Vulnerable and Cautious Traditionalists clusters. This misalignment between perceived and actual knowledge could make this group particularly vulnerable to financial missteps or exploitation in digital financial environments.

The Digitally Hesitant At-Risk group shows a polarized distribution of self-perceived knowledge. While they have the highest proportion rating their knowledge as very low or quite low (27%), they also have a notable proportion (22%) rating their knowledge as quite high or very high. This polarization might reflect diverse subgroups within this cluster or could indicate varying levels of awareness about their financial vulnerabilities.

These findings highlight the interesting relationship between perceived and actual financial knowledge, which underscores the importance of targeted financial education that not only improves objective knowledge but also helps individuals accurately assess their own financial literacy. This self-awareness is crucial in the context of cybersecurity, as overconfidence in financial matters could lead to increased vulnerability to sophisticated financial scams or cyber threats.

4.3. Financial Decision Making Across Clusters

As regards financial decision making, the Cyber-Savvy Pragmatists and Digital-Savvy Vulnerable groups show very similar patterns, with approximately 55% of individuals making financial decisions independently and 44% making decisions jointly with someone else (see Figure 3). This relatively high level of personal involvement in financial decision making aligns well with their digital savviness and, in the case of Cyber-Savvy Pragmatists, their high financial knowledge. The similarity between these two groups suggests that digital comfort may be a key factor in promoting individual financial autonomy, regardless of overall financial vulnerability.

Cautious Traditionalists present an interesting contrast, with the highest proportion (51%) making financial decisions jointly with someone else. This could reflect a more conservative approach to financial management, possibly rooted in traditional family structures or a preference for shared responsibility in financial matters. Their lower rate of independent decision making (46%) might also be linked to their lower digital comfort, potentially leading them to seek input from others more frequently.

The Comfortably Naive cluster shows a relatively balanced distribution between independent (50%) and joint (47%) decision making. This pattern, combined with their high financial stability but low financial knowledge, suggests that while they feel comfortable making decisions, they may also recognize the value of consulting others, possibly as a way to compensate for their lack of financial acumen.

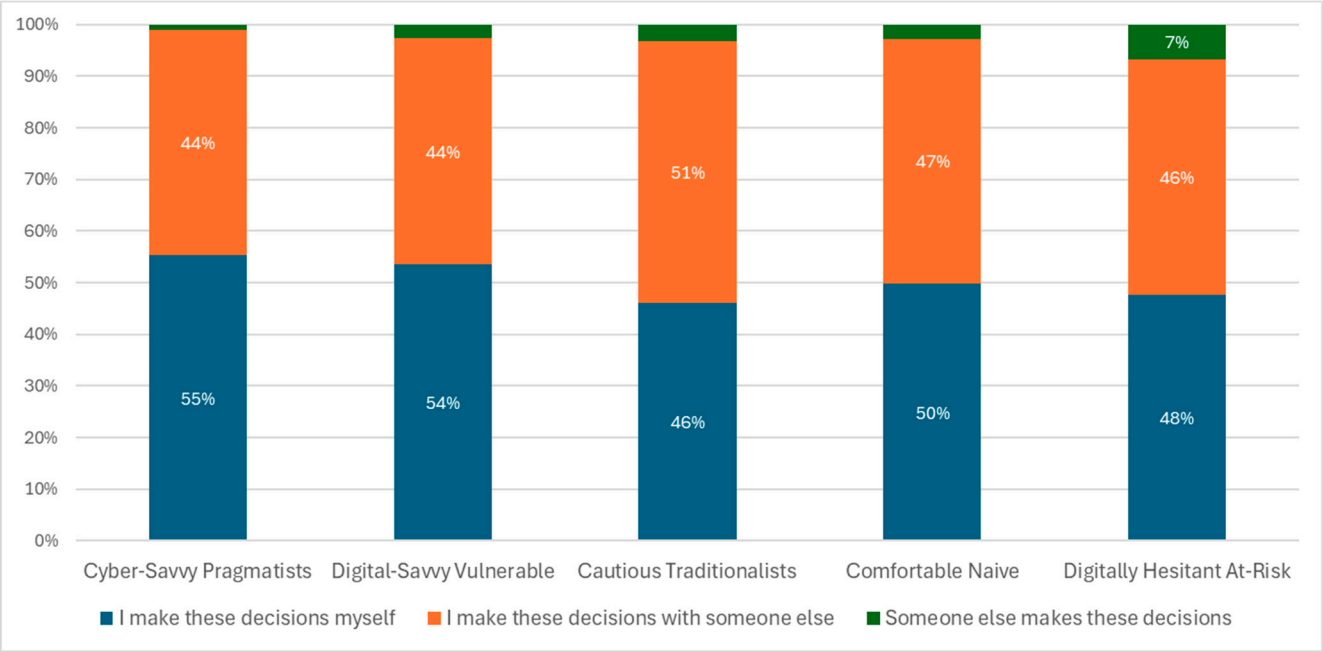


Figure 3. Financial decision-making patterns across cyber-financial risk profiles. This graph shows the percentage of individuals within each cluster who make financial decisions independently, jointly with someone else, or delegate decisions to others. These patterns reveal how different risk profiles associate with varying levels of financial autonomy and collaborative decision making. Data source: Flash Eurobarometer 525 survey, 2023.

The Digitally Hesitant At-Risk group presents the most diverse distribution, with the lowest rate of independent decision making (48%) and the highest rate of delegating decisions to others (7%). This pattern aligns with their overall risk profile, suggesting that their low financial knowledge and digital hesitancy may lead them to feel less confident in making financial decisions independently. The higher rate of delegating decisions could indicate a recognition of their limitations or possibly a lack of engagement with financial matters.

Across all clusters, joint decision making represents a significant proportion (between 44% and 51%), highlighting the collaborative nature of household financial management for many Europeans. This trend towards shared responsibility could be seen as a positive factor, potentially leading to more balanced and considered financial choices. The generally low percentages of individuals who completely delegate financial decisions to others (ranging from 1% to 7%) indicate that most people, regardless of their financial literacy or digital comfort, maintain some level of involvement in their financial affairs. However, the higher rate among the Digitally Hesitant At-Risk group (7%) flags a potential vulnerability that may need addressing through targeted financial empowerment initiatives.

4.4. Socio-Economic Risk Profiles

The gender distribution across cyber-financial risk profiles reveals a striking pattern that underscores the relevance of gender in understanding and addressing digital financial vulnerabilities (see Figure 4).

At one end of the spectrum, we see a male-dominated Cyber-Savvy Pragmatist group (61% male), characterized by high financial knowledge and digital comfort. This contrasts sharply with the female-majority clusters at the other end, particularly the Comfortably Naive (60% female) and Digitally Hesitant At-Risk (63% female) groups, which exhibit lower financial knowledge or digital comfort, or both. The middle ground, represented by the Digital-Savvy Vulnerable individuals and Cautious Traditionalists, shows a more balanced gender distribution. This overall pattern suggests a gender gap in cyber-financial

resilience, with women disproportionately represented in higher-risk categories. Such a disparity points to potential underlying factors including differences in financial education, digital literacy, economic opportunities, or social norms that shape financial behaviors and risk exposure.

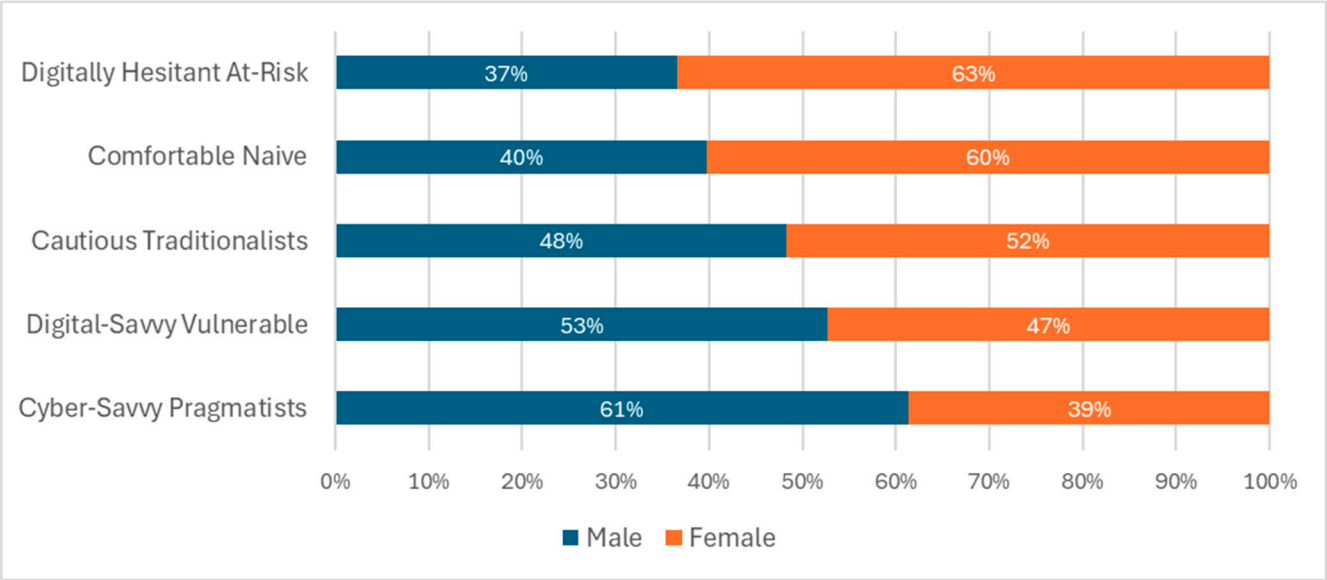


Figure 4. Gender distribution within cyber-financial risk profiles. This graph shows the percentage of males and females in each cluster, revealing significant gender disparities across different risk profiles, particularly in the Cyber-Savvy Pragmatist (male-dominated) and Digitally Hesitant At-Risk (female-dominated) groups. Data source: Flash Eurobarometer 525 survey, 2023.

While age differences are not particularly pronounced, they do offer additional context for understanding the vulnerabilities and strengths of each group. Cyber-Savvy Pragmatists show a skew towards older age groups, with nearly half (48%) aged 55 and above. This suggests that their high financial knowledge and stability may be partly attributed to life experience and accumulated wealth. However, their digital comfort despite an older age profile indicates successful adaptation to technological changes.

The Digital-Savvy Vulnerable cluster has a more balanced age distribution, with a slight tilt towards younger and middle-aged individuals. The higher representation in the 25–54 age range (49%) aligns with their digital comfort but may also explain their financial vulnerability, as they might be in career-building or family-raising stages with higher expenses and financial pressures.

Cautious Traditionalists show the strongest bias towards older age groups, with 49% aged 55 and above. This corresponds well with their low digital comfort and moderate financial stability, suggesting a more traditional approach to financial management that may be rooted in long-standing habits.

The Comfortably Naive cluster presents a relatively even distribution across age groups, with a slight increase in the 65 and older category. This even spread indicates that financial naivety coupled with comfort can occur across generations, highlighting the importance of financial education at all life stages (See Figure 5).

Digitally Hesitant At-Risk individuals show a more pronounced representation in younger age groups, with 51% under 45. This younger skew, combined with their risk profile, suggests that this group may face challenges in establishing financial stability and literacy early in their adult lives, potentially setting the stage for long-term financial vulnerability if not addressed.

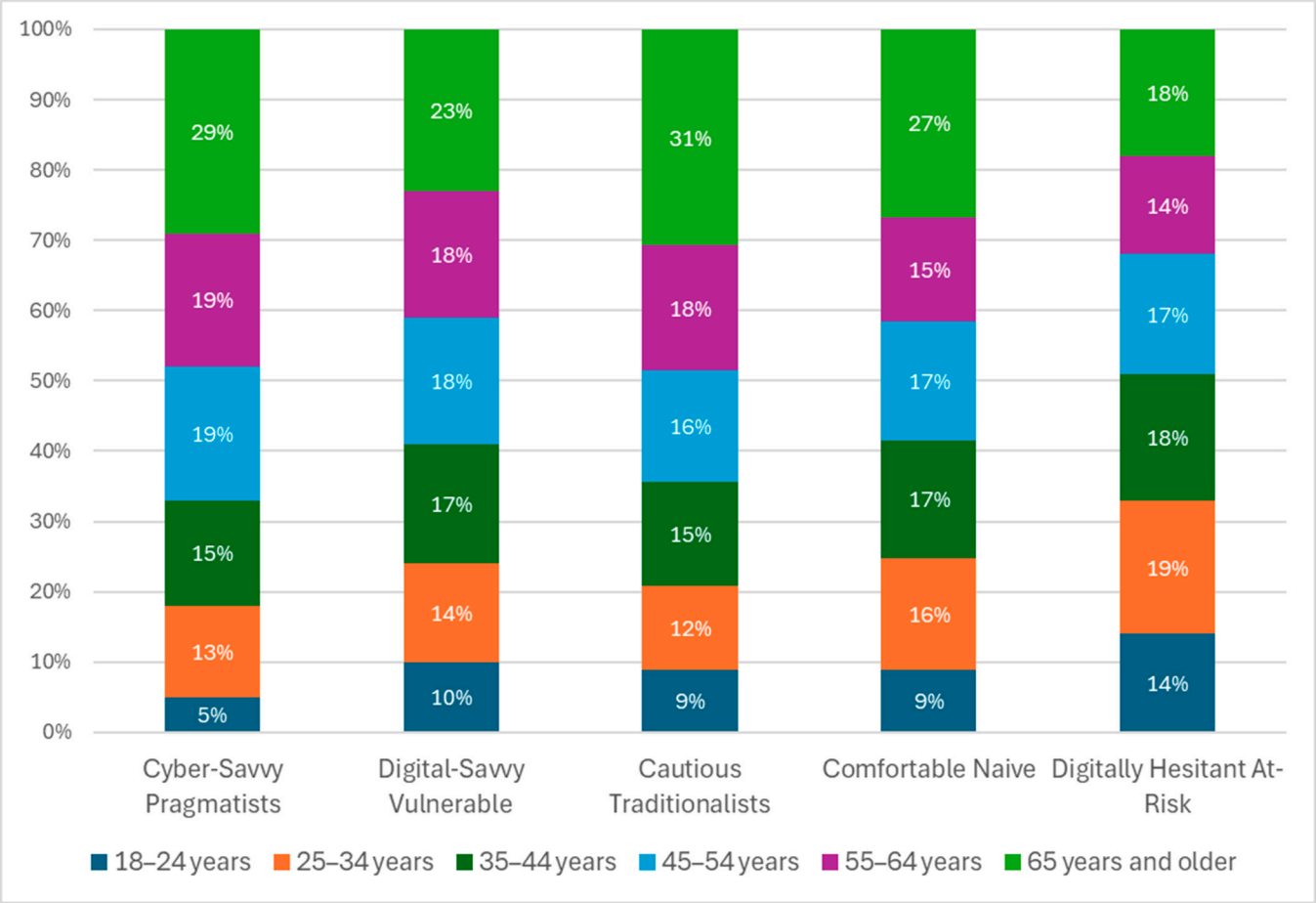


Figure 5. Age distribution across cyber-financial risk profiles. This graph shows the percentage of individuals in different age groups (18–24, 25–34, 35–44, 45–54, 55–64, and 65+) within each cluster, illustrating how age relates to different combinations of financial knowledge, vulnerability, and digital comfort. Data source: Flash Eurobarometer 525 survey, 2023.

We also notice a relationship between education levels and cyber-financial risk profiles (see Figure 6). Education levels in our analysis were categorized into three broad groups following standard ISCED (International Standard Classification of Education) conventions. Low education encompasses individuals with no formal education, primary education, and lower secondary education (including those who completed compulsory education up to approximately age 14). Medium education includes upper secondary education (both general and vocational tracks), post-secondary non-tertiary education, and various forms of vocational training that do not lead to a tertiary degree. High education comprises all tertiary education levels, from short-cycle tertiary programs through bachelor's and master's degrees to doctoral studies. In our sample, 20.3% of respondents had low education, 48.2% medium education, and 31.5% high education.

Cyber-Savvy Pragmatists stand out with the highest proportion of highly educated individuals (45%) and the lowest percentage of those with low education (13%). This aligns well with their high financial knowledge scores and digital comfort, suggesting that formal education may contribute to their overall financial literacy and technological adaptability. Their educational background likely equips them with critical thinking skills that aid in navigating continually changing financial landscapes and recognizing sophisticated cyber threats.

The Digital-Savvy Vulnerable cluster shows a more moderate educational profile, with 30% highly educated and a majority (53%) with medium education. This distribution reflects their moderate financial knowledge and high digital comfort. However, their

financial vulnerability despite this educational background highlights that formal education alone may not guarantee financial stability, particularly in the face of economic pressures or life circumstances.

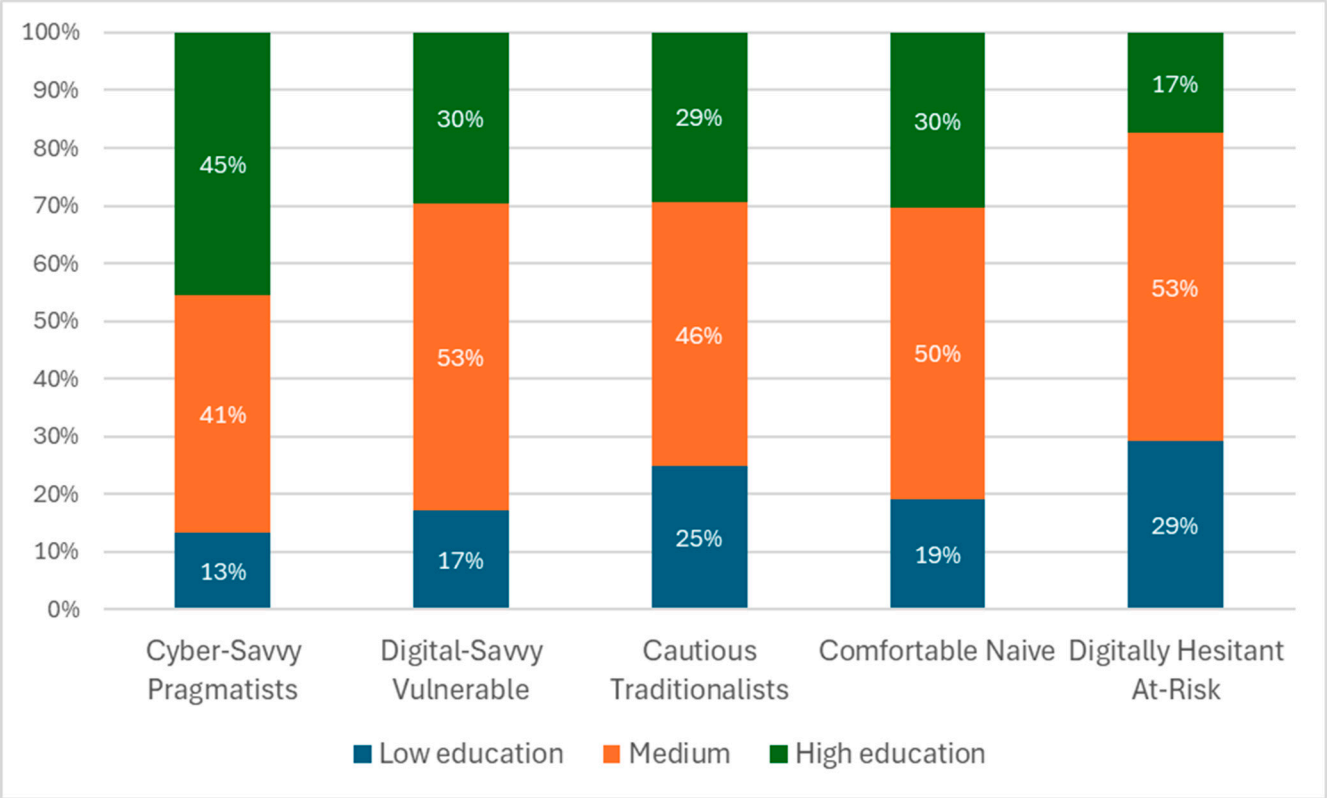


Figure 6. Educational attainment across cyber-financial risk profiles. This graph shows the distribution of education levels (low, medium, and high) within each cluster, revealing how educational background relates to different patterns of financial knowledge, vulnerability, and digital comfort. Data source: Flash Eurobarometer 525 survey, 2023.

Cautious Traditionalists present a slightly lower educational profile, with 29% highly educated and a quarter (25%) with low education. This distribution correlates with their lower digital comfort and moderate financial knowledge, suggesting that their cautious approach to digital financial services may be partly influenced by educational background. Their moderate financial stability despite lower education levels indicates that traditional financial wisdom and conservative practices can sometimes compensate for formal financial education.

The Comfortably Naive cluster mirrors the Digital-Savvy Vulnerable one in terms of high education (30%) but with a slightly higher proportion of medium education (50%). This profile presents an intriguing contrast with their very low financial knowledge, indicating that general education does not necessarily translate to financial literacy. Their comfort with digital services, coupled with financial naivety across education levels, underscores the need for specific financial education, regardless of overall educational attainment.

Digitally Hesitant At-Risk individuals show the lowest proportion of high education (17%) and the highest of low education (29%). This educational profile aligns with their low financial knowledge and high vulnerability, suggesting a compounding effect where lower educational attainment may contribute to both reduced financial literacy and limited digital skills. However, the majority still falling in the medium education category (53%) indicates that factors beyond formal education play a significant role in their financial vulnerability and digital hesitancy.

4.5. Regional Risk Profiles

In Western Europe, the Netherlands and Denmark stand out with high proportions of Cyber-Savvy Pragmatists (47% and 43%, respectively). This aligns with these countries' reputation for strong digital infrastructure and financial literacy (see Table 3 and Figure 7).

Table 3. Distribution of cyber-financial risk profiles across EU member states. This table shows the percentage of each country's population falling into the five identified risk clusters: Cyber-Savvy Pragmatists (high financial knowledge and digital comfort), Digital-Savvy Vulnerable individuals (moderate knowledge but financially vulnerable), Cautious Traditionalists (moderate knowledge and low digital comfort), Comfortably Naive individuals (low knowledge and high digital comfort), and Digitally Hesitant At-Risk individuals (low knowledge and high vulnerability). Data source: Flash Eurobarometer 525 survey, 2023.

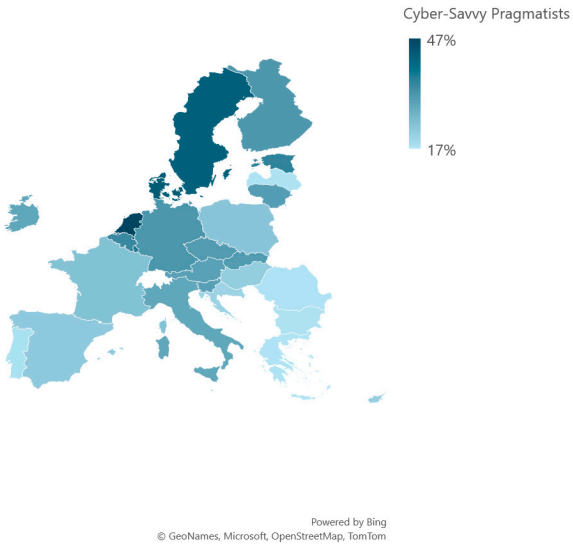
	Digitally Hesitant At-Risk Individuals	Cyber-Savvy Pragmatists	Digital-Savvy Vulnerable Individuals	Cautious Traditionalists	Comfortably Naive Individuals	Digitally Hesitant At-Risk Individuals
Austria	18%	30%	18%	13%	22%	18%
Belgium	21%	34%	11%	13%	20%	21%
Bulgaria	26%	17%	18%	16%	22%	26%
Croatia	21%	20%	21%	14%	24%	21%
Cyprus	27%	21%	15%	15%	21%	27%
Czech Republic	21%	31%	19%	10%	19%	21%
Denmark	14%	43%	18%	8%	16%	14%
Estonia	13%	36%	24%	13%	14%	13%
Finland	15%	32%	37%	6%	11%	15%
France	22%	24%	13%	21%	20%	22%
Germany	19%	32%	15%	15%	19%	19%
Greece	30%	17%	15%	21%	17%	30%
Hungary	20%	21%	21%	18%	20%	20%
Italy	22%	29%	10%	20%	20%	22%
Latvia	30%	17%	22%	14%	17%	30%
Lithuania	18%	30%	17%	10%	25%	18%
Luxembourg	11%	38%	11%	14%	27%	11%
Malta	17%	30%	17%	13%	23%	17%
Netherlands	13%	47%	12%	9%	19%	13%
Poland	24%	23%	18%	13%	23%	24%
Portugal	26%	18%	13%	21%	23%	26%
Republic of Ireland	21%	29%	16%	16%	18%	21%
Romania	32%	17%	13%	12%	26%	32%
Slovakia	20%	31%	18%	10%	21%	20%
Slovenia	15%	30%	24%	17%	14%	15%
Spain	19%	22%	13%	24%	22%	19%
Sweden	13%	42%	15%	8%	23%	13%

Sweden follows closely behind with 42% in this category, forming a cluster of Nordic countries with high financial and digital competence. France presents a more balanced distribution across all clusters, with a slight edge in Cyber-Savvy Pragmatists (24%). This

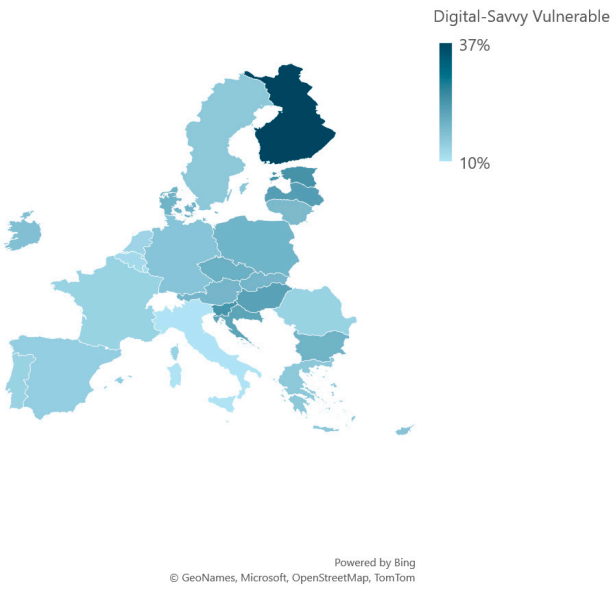
even spread might reflect the diverse economic landscape and varying levels of financial engagement across different segments of French society. Germany shows a skew towards Cyber-Savvy Pragmatists (32%), but also has significant representations in other categories, suggesting a heterogeneous financial landscape that caters to different levels of financial sophistication.

Southern European countries show distinct patterns. Greece and Portugal have higher proportions of Digitally Hesitant At-Risk individuals (30% and 26%, respectively), possibly reflecting the lingering effects of economic challenges and slower digital adoption in the financial sector. Italy shows a more balanced distribution, with a lean towards Cyber-Savvy Pragmatists (29%), indicating a potentially more diverse financial ecosystem.

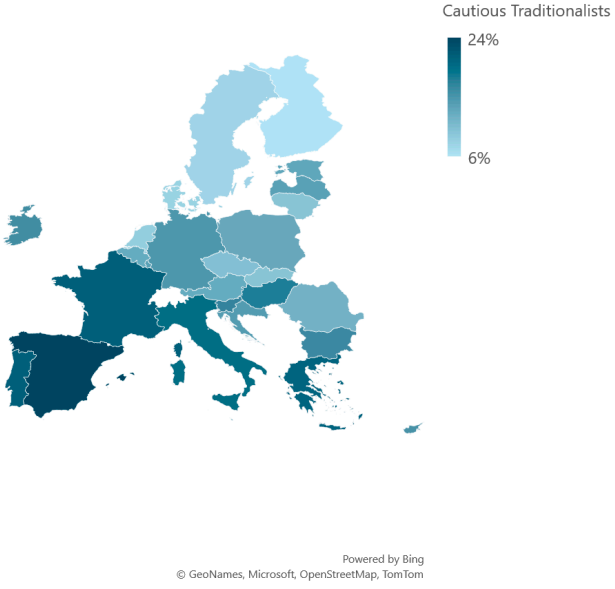
Eastern European countries present varied profiles. Estonia stands out with a high proportion of Cyber-Savvy Pragmatists (36%) and Digital-Savvy Vulnerable individuals (24%), suggesting rapid digital adoption but potential economic vulnerabilities. In contrast, Romania has the highest proportion of Digitally Hesitant At-Risk individuals (32%), possibly indicating challenges in financial inclusion and digital literacy.



(**a**) Country distribution of Cyber-Savvy Pragmatists

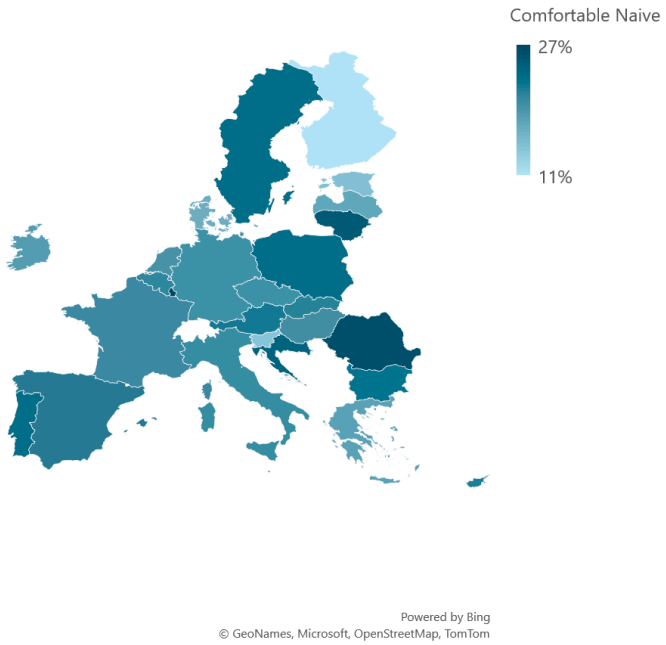


(**b**) Country distribution of Digital-Savvy Vulnerable individuals

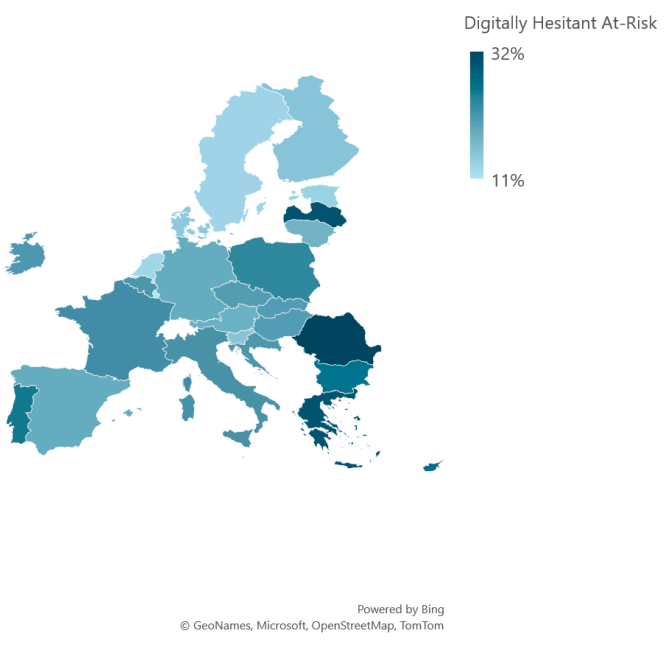


(**c**) Country distribution of Cautious Traditionalists

Figure 7. *Cont.*



(**d**) Country distribution of Comfortably Naive individuals



(**e**) Country distribution of Digitally Hesitant At-Risk individuals

Figure 7. Geographic distribution of cyber-financial risk profiles across European Union member states. These five maps show the relative prevalence of each risk profile: (**a**) Cyber-Savvy Pragmatists, characterized by high financial knowledge and digital comfort; (**b**) Digital-Savvy Vulnerable individuals, showing moderate knowledge but high financial vulnerability; (**c**) Cautious Traditionalists, with moderate knowledge but low digital comfort; (**d**) Comfortably Naive individuals, displaying high digital comfort but low financial knowledge; and (**e**) Digitally Hesitant At-Risk individuals, characterized by low knowledge and high vulnerability. Darker shades indicate higher prevalence of each profile. Data source: Flash Eurobarometer 525 survey, 2023.

Finland presents an intriguing outlier case with the highest proportion of Digital-Savvy Vulnerable individuals (37%) among all countries. This unique profile suggests a population comfortable with digital finance but potentially facing economic pressures or lacking comprehensive financial knowledge.

The Baltic states show varied profiles, with Latvia having a high proportion of Digitally Hesitant At-Risk individuals (30%), while Lithuania has a more balanced distribution, leaning towards Cyber-Savvy Pragmatists (30%) and Comfortably Naive individuals (25%).

Central European countries like Austria, Czech Republic, and Slovakia show relatively balanced distributions, with a tilt towards Cyber-Savvy Pragmatists, suggesting steady progress in financial literacy and digital adoption.

5. Discussion

Our identification of cyber-financial risk profiles provides useful information about the cybersecurity landscape across Europe, identifying distinctive patterns of financial literacy, digital comfort, and economic vulnerability. These profiles offer a better understanding of how different segments of the European population may be susceptible to various cyber threats, particularly in the realm of digital finance. The five distinct clusters, namely, Cyber-Savvy Pragmatists, Digital-Savvy Vulnerable individuals, Cautious Traditionalists, Comfortably Naive individuals, and Digitally Hesitant At-Risk individuals, highlight that cybersecurity vulnerabilities in Europe are not uniform. Each group presents specific challenges and potential entry points for cybercriminals, necessitating tailored cybersecurity strategies.

A significant finding of our analysis is the discrepancy between digital comfort and financial knowledge, particularly evident in the Comfortably Naive cluster. This gap

highlights a substantial cybersecurity risk, as individuals who are comfortable with digital platforms but lack financial acumen may be prime targets for sophisticated phishing attacks, investment scams, or identity theft schemes. These threats exploit users' confidence in navigating online environments, coupled with their limited understanding of financial intricacies.

The identification of the Digital-Savvy Vulnerable cluster also highlights an interesting category of users who, despite their digital comfort, remain financially vulnerable. This group may be particularly susceptible to novel cyber threats that exploit the intersection of digital savviness and financial pressure, such as fraudulent quick-loan schemes or cryptocurrency scams. This finding points to the need for cybersecurity measures that not only address technical vulnerabilities but also consider the financial circumstances of users.

The analysis of self-perceived financial knowledge across cyber-financial risk profiles has implications for cybersecurity and financial literacy efforts. While Cyber-Savvy Pragmatists demonstrate a good alignment between perceived and actual financial knowledge, other clusters show varying degrees of mismatch. Notably, the Comfortably Naive cluster exhibits a tendency to overestimate their financial acumen. This overconfidence, combined with low objective financial knowledge, could make them vulnerable to sophisticated financial scams and cyber threats. Conversely, Cautious Traditionalists show a more conservative self-assessment, which aligns with their hesitancy towards digital financial tools. The Digital-Savvy Vulnerable and Digitally Hesitant At-Risk groups present mixed patterns, with the latter showing a polarized distribution of self-perceived knowledge.

The prevalence of joint financial decision making across all clusters suggests a potential avenue for enhancing cybersecurity. Encouraging collaborative approaches to digital financial management could serve as an additional layer of security, particularly for more vulnerable groups. This finding highlights the potential role of social dynamics in strengthening cyber resilience.

The clear gender disparity across clusters, with women over-represented in higher-risk categories, points to a potential gender gap in cybersecurity resilience. This finding shows the need for targeted cybersecurity education and awareness programs that address gender-specific vulnerabilities and behaviors in digital financial ecosystems. Similarly, while age differences across clusters were not stark, the educational disparities highlight the role of formal education in shaping cyber-financial resilience. However, the presence of financially naive individuals across education levels emphasizes that specialized financial and digital literacy education is important for enhancing cybersecurity, regardless of general educational attainment.

Regional variations in the distribution of risk profiles across European countries reveal significant disparities in cyber-financial resilience. Countries with higher proportions of Cyber-Savvy Pragmatists, such as the Netherlands and Nordic countries, may have more robust defenses against financial cyber threats. In contrast, regions with larger shares of Digitally Hesitant At-Risk individuals, like some Southern and Eastern European countries, may face heightened cybersecurity challenges in the financial sector. These regional differences call for tailored approaches to cybersecurity that account for local contexts and vulnerabilities.

5.1. Contributions to the State of the Art

Cyber-Savvy Pragmatists, characterized by high financial knowledge and digital comfort, align with findings from studies like Lee and Kim (2020), who found that individuals with higher technological competencies are better equipped to protect themselves against cyber threats. However, our research extends this understanding by highlighting that even this group may face sophisticated phishing attempts or APTs, echoing concerns raised by Abroshan et al. (2021) about the persistent vulnerability to phishing across different groups.

The Digital-Savvy Vulnerable cluster presents an interesting paradox. While their digital comfort aligns with positive cybersecurity outcomes suggested by some studies (e.g., Lee and Kim 2020), their financial vulnerability introduces a new dimension of risk. This

finding supports and extends the work of Houtti et al. (2024), who found that countries with a lower GNI per capita are more vulnerable to scams, by showing how individual-level financial vulnerability interacts with digital savviness to create a unique risk profile.

Our findings also shed light on the complicated and often inverse relationship between cybersecurity measures and financial accessibility. As cybersecurity protocols become more stringent—with multi-factor authentication, complex password requirements, and sophisticated verification processes—they can inadvertently create barriers to financial-services access, particularly for less digitally confident users. This inverse relationship is especially evident in our Digital-Savvy Vulnerable cluster, where users must balance security requirements with financial needs. Enhanced security measures, while necessary, can increase transaction friction, potentially leading some users to seek less secure but more convenient alternatives. Additionally, the costs associated with implementing robust cybersecurity measures may be passed on to consumers, creating financial barriers that particularly affect vulnerable populations. This tension between security and accessibility indicates a need for balanced approaches that protect users while maintaining financial inclusion, supporting previous findings by Ahmed et al. (2024) on the delicate balance between auxiliary innovation and customer protection in digital banking.

The Cautious Traditionalists in our study share characteristics with groups identified in previous research as potentially vulnerable due to lower digital engagement. This aligns with findings from Koskelainen et al. (2023), who emphasized the need for digital financial literacy in addition to traditional financial knowledge. Our research shows how moderate financial stability might partially offset risks associated with low digital comfort.

The Comfortably Naive cluster presents a profile that is particularly concerning in light of the existing literature. Their high digital comfort coupled with low financial knowledge creates a risk profile that aligns with Whitty's (2019) findings on the role of overconfidence in increasing susceptibility to cyber-fraud. This group exemplifies the dangers highlighted by Rey-Ares et al. (2024), who found that both objective and subjective financial knowledge could increase exposure to fraudulent emails.

The Digitally Hesitant At-Risk group in our study corresponds closely to the high-risk profiles identified in much of the existing literature. Their low financial knowledge and high vulnerability align with factors that Judges (2021) and others have associated with increased susceptibility to scams and fraud.

Our findings also extend the work of Whitty (2019) on the role of overconfidence in cyber-fraud susceptibility by providing a more nuanced understanding of how this overconfidence manifests across different risk profiles.

The clear gender disparity across our identified clusters, with women over-represented in higher-risk categories, adds to the existing literature on gender and cybersecurity. While some studies, like Abroshan et al. (2021), found that women were more likely to click on phishing links, our research suggests that gender differences in cyber-financial risks are more complicated and intersect with factors like financial knowledge and digital comfort. This finding highlights the need for a more systematic approach to understanding gender disparities in cybersecurity, as suggested by Wei et al. (2024).

Our findings on age and education distributions across clusters also add to the understanding offered by existing studies. While we found some alignment with research like Judges (2021) and Whitty (2019) regarding older adults' vulnerabilities, our results suggest that age-related risks are not uniform and interact with financial knowledge and digital comfort. Similarly, our findings on education levels support but also complicate the general association between higher education and better cybersecurity practices noted by Isa et al. (2021) and Wei et al. (2024), by showing how education interacts with other factors to produce varied risk profiles.

The regional variations in risk profile distribution that we identified extend the work of researchers like Lee and Kim (2020) on country-level cybersecurity preparedness. Our findings provide a more granular view of how cyber-financial risks vary across European

countries, highlighting the need for tailored, region-specific approaches to cybersecurity policy and education.

5.2. Research Limitations and Directions for Future Studies

The cross-sectional nature of the Flash Eurobarometer 525 data limits our ability to observe changes in risk profiles over time or in response to specific events or interventions. Future longitudinal studies could address this limitation by tracking individuals' cyber-financial risk profiles over extended periods, allowing for the examination of temporal trends and causal relationships.

The reliance on self-reported data for digital comfort may introduce biases, as respondents might overestimate or underestimate their capabilities. Future research could benefit from incorporating objective measures of digital skills to complement self-reported data.

This study's focus on three key dimensions, while providing a comprehensive overview, may not capture all relevant factors contributing to cyber-financial risk. Additional variables, such as specific online behaviors, exposure to cybersecurity education, or experiences with financial fraud, could provide a deeper understanding of risk profiles. This research also does not directly measure actual cybersecurity outcomes or incidents, which limits our ability to validate the real-world implications of the identified risk profiles. Incorporating data on cybersecurity breaches or financial fraud victimization could strengthen the practical relevance of the risk profiles.

Lastly, the rapid evolution of digital financial services and cybersecurity threats means that the relevance of specific risk factors may change over time. Regular updates to the risk profile framework and continuous monitoring of emerging trends in digital finance and cybersecurity would be necessary to maintain the applicability of these findings in a fast-changing digital landscape.

5.3. Policy Implications

Based on the findings presented in our study, we can formulate several important policy implications for addressing cyber-financial risks and enhancing cybersecurity across Europe. The identification of distinct cyber-financial risk profiles underscores the need for targeted approaches to cybersecurity policy rather than one-size-fits-all solutions. Policymakers should consider developing stratified cybersecurity awareness campaigns and educational programs that address the specific vulnerabilities of each identified group.

For the Comfortably Naive cluster, who demonstrate high digital comfort but low financial knowledge, policies should focus on integrating financial literacy education with cybersecurity training. This could involve mandating financial institutions to provide user-friendly educational materials on potential cyber threats alongside their digital services. The overconfidence observed in this group suggests that interventions should not only impart knowledge but also cultivate a realistic self-assessment of one's financial acumen and cyber risks.

The gender disparity revealed in the risk profiles calls for gender-sensitive cybersecurity policies. Initiatives to increase women's participation in financial decision making and enhance their digital literacy could help bridge this gap. This might include targeted outreach programs, mentorship initiatives, and the promotion of female role models in finance and technology sectors.

For regions with high proportions of Digitally Hesitant At-Risk individuals, policies should prioritize basic digital literacy alongside cybersecurity education. This could involve public–private partnerships to provide free or subsidized digital skills training, with a strong emphasis on safe online financial practices. Additionally, regulations could require financial service providers to implement extra security measures and simplified interfaces for users identified as potentially vulnerable.

The prevalence of joint financial decision making across all clusters suggests that policymakers should consider family-oriented cybersecurity initiatives. This could in-

clude promoting 'cyber-safety discussions' within households and providing resources for families to collectively enhance their digital financial security.

Given the rapid evolution of cyber threats, policies should also focus on creating adaptive regulatory frameworks that can quickly respond to emerging risks in the digital financial landscape. This might involve establishing cross-border co-operation mechanisms for sharing threat intelligence and best practices in cyber-financial security across EU member states.

Lastly, the regional variations in risk profiles highlight the need for EU-level policies that address disparities in cyber-financial resilience while allowing for country-specific implementations. This could involve setting minimum standards for cyber-financial education across the EU, coupled with targeted support for countries with higher proportions of at-risk populations.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/risks12120200/s1, Supplementary Material detailing the validation of the cluster analysis.

Author Contributions: Conceptualization, A.R.C., R.R., D.Ț. and A.R.; data curation, R.R. and A.R.; formal analysis, A.R.C., R.R. and D.Ț.; investigation, A.R.C., R.R. and A.R.; methodology, A.R.C., R.R., D.Ț. and A.R.; project administration, R.R. and D.Ț.; resources, R.R. and D.Ț.; supervision, R.R. and D.Ț.; validation, A.R.C., R.R. and D.Ț.; visualization, R.R. and D.Ț.; writing—original draft, A.R.C., R.R., D.Ț. and A.R.; writing—review and editing, A.R.C., R.R., D.Ț. and A.R. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are publicly available in the GESIS ZACAT repository (European Commission 2023b).

Conflicts of Interest: The authors declare no conflicts of interest.

References

Abdulai, Mohammed A. 2020. Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology* 14: 157–74.

Abroshan, Hossein, Jan Devos, Geert Poels, and Eric Laermans. 2021. Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access* 9: 44928–49. [CrossRef]

Ahmed, Faraz, Arsalan Hussain, Sajjad Nawaz Khan, Arsalan Haneef Malik, Muhammad Asim, Sadique Ahmad, and Mohammed El-Affendi. 2024. Digital Risk and Financial Inclusion: Balance Between Auxiliary Innovation and Protecting Digital Banking Customers. *Risks* 12: 133. [CrossRef]

Al-Kumaim, Nabil Hasan, and Sultan Khalifa Alshamsi. 2023. Determinants of cyberattack prevention in UAE financial organizations: Assessing the mediating role of cybersecurity leadership. *Applied Sciences* 13: 5839. [CrossRef]

Amnas, Muhammed Basid, Murugesan Selvam, and Satyanarayana Parayitam. 2024. FinTech and Financial Inclusion: Exploring the Mediating Role of Digital Financial Literacy and the Moderating Influence of Perceived Regulatory Support. *Journal of Risk and Financial Management* 17: 108. [CrossRef]

Bran, Emanuela, Cosima Rughiniș, Gheorghe Nadoleanu, and Michael G. Flaherty. 2023. The emerging social status of generative AI: Vocabularies of ai competence in public discourse. Paper presented at the 2023 24th International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, May 24–26; pp. 391–98.

Broadhurst, Roderic, Katie Skinner, Nicholas Sifniotis, Bryan Matamoros-Macias, and Yuguang Ipsen. 2019. Phishing and cybercrime risks in a university student community. *International Journal of Cybersecurity Intelligence & Cybercrime* 2: 4–23.

European Commission. 2023a. Flash Eurobarometer 525 "Monitoring the Level of Financial Literacy in the EU" Report. Available online: https://op.europa.eu/en/publication-detail/-/publication/b92b197d-4098-11ee-952f-01aa75ed71a1/language-en (accessed on 2 September 2024).

European Commission. 2023b. Flash Eurobarometer 525 (Monitoring the Level of Financial Literacy in the EU). GESIS, Cologne. ZA7985 Data File Version 1.0.0. Available online: https://search.gesis.org/research_data/ZA7985 (accessed on 2 September 2024).

Guedes, Inês, Margarida Martins, and Carla Sofia Cardoso. 2023. Exploring the determinants of victimization and fear of online identity theft: An empirical study. *Security Journal* 36: 472–97. [CrossRef]

Hossain, Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, and Yue Xu. 2024. Local government cybersecurity landscape: A systematic review and conceptual framework. *Applied Sciences* 14: 5501. [CrossRef]

Houtti, Mo, Abhishek Roy, Venkata Narsi Reddy Gangula, and Ashley Marie Walker. 2024. A Survey of Scam Exposure, Victimization, Types, Vectors, and Reporting in 12 Countries. *arXiv* arXiv:2407.12896.

Isa, Mohd Yaziz Bin Mohd, Wan Nora Binti Wan Ibrahim, and Zulkifflee Mohamed. 2021. The Relationship Between Financial Literacy and Public Awareness on Combating the Threat of Cybercrime in Malaysia. *The Journal of Industrial Distribution & Business* 12: 1–10.

Judges, Rebecca. 2021. Scams and Aging: Factors Impacting Effective Decision Making. Ph.D. thesis, University of Toronto, Toronto, ON, Canada.

Koskelainen, Tiina, Panu Kalmi, Eusebio Scornavacca, and Tero Vartiainen. 2023. Financial literacy in the digital age—A research agenda. *Journal of Consumer Affairs* 57: 507–28. [CrossRef]

Kovács, Levente, and Elemér Terták. 2024. Financial Literacy is the Best Protection from Cybercrime. *Economy and Finance: English-Language Edition of Gazdaság és Pénzügy* 11: 7–28. [CrossRef]

Lee, Claire Seungeun, and Ji Hye Kim. 2020. Latent groups of cybersecurity preparedness in Europe: Sociodemographic factors and country-level contexts. *Computers & Security* 97: 101995.

Mishra, Shailendra. 2023. Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences* 13: 5875. [CrossRef]

Rey-Ares, Lucía, Sara Fernández-López, and Marcos Álvarez-Espiño. 2024. The role of financial literacy in consumer financial fraud exposure (via email) and victimisation: Evidence from Spain. *International Journal of Bank Marketing* 42: 1388–413. [CrossRef]

Ribeiro, Liliana, Inês Sousa Guedes, and Carla Sofia Cardoso. 2024. Which factors predict susceptibility to phishing? An empirical study. *Computers & Security* 136: 103558.

Rughiniş, Cosima, and Michael G. Flaherty. 2022. The social bifurcation of reality: Symmetrical construction of knowledge in science-trusting and science-distrusting discourses. *Frontiers in Sociology* 7: 782851. [CrossRef] [PubMed]

Rughiniș, Cosima, Simona-Nicoleta Vulpe, Michael G. Flaherty, and Sorina Vasile. 2022. Shades of doubt: Measuring and classifying vaccination confidence in Europe. *Vaccine* 40: 6670–79. [CrossRef] [PubMed]

Sheng, Steve, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Paper presented at the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GA, USA, April 10–15; pp. 373–82.

Vulpe, Simona-Nicoleta, and Cosima Rughiniş. 2021. Social amplification of risk and "probable vaccine damage": A typology of vaccination beliefs in 28 European countries. *Vaccine* 39: 1508–15. [CrossRef] [PubMed]

Wei, Miranda, Jaron Mink, Yael Eiger, Tadayoshi Kohno, Elissa M. Redmiles, and Franziska Roesner. 2024. SoK (or SoLK?): On the Quantitative Study of Sociodemographic Factors and Computer Security Behaviors. *arXiv* arXiv:2404.10187.

Whitty, Monica T. 2019. Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime* 26: 277–92. [CrossRef]