systems

MDPI

*Article*

# The Economic Dimension of Cybercrime in the Digital Era: A Systems Perspective on Structural Inequalities and Regional Dynamics of Computer Fraud in Spain

**Carlos J. Mármol, Aurelio Luna and Isabel Legaz ***

Department of Legal and Forensic Medicine, Biomedical Research Institute of Murcia (IMIB), Regional Campus of International Excellence "Campus Mare Nostrum", Faculty of Medicine, University of Murcia (UMU), 30100 Murcia, Spain; cj.marmol@um.es (C.J.M.); aurluna@um.es (A.L.)
* Correspondence: isalegaz@um.es; Tel.: +34-868883957; Fax: +34-868834307

**Abstract**

Computer fraud has become a rapidly expanding form of cybercrime linked to the growth of digital infrastructures and socioeconomic development. This study adopts a socio-technical systems perspective to examine the temporal evolution, regional disparities, structural determinants, and future trends of computer fraud in Spain (2011–2022). Official data from the Spanish Ministry of the Interior were used to calculate incidence rates per 100,000 inhabitants. Temporal trends were analyzed using linear regression, regional patterns using clustering analysis, and structural associations using correlation models. Projections were developed to estimate trends up to 2035. Computer fraud increased sharply from 44.7 to 707.7 cases per 100,000 inhabitants, with the strongest growth observed in card and bank fraud. Higher rates were found in economically developed and highly digitalized regions. Fraud incidence was positively associated with broadband access, mobile connectivity, and income levels, whereas traditional technologies were negatively associated. These findings indicate that computer fraud should be understood as a system-level phenomenon driven by the interplay of digital, economic, and territorial factors. Effective prevention requires integrated strategies that combine technological, regulatory, and educational measures, adapted to regional vulnerability profiles.

**Keywords:** computer fraud; cybercrime; digital economy; regional disparities; socio-technical systems; systemic risk

Check for updates

Academic Editors: Uchenna Daniel Ani and Hongmei He

Received: 20 March 2026
Revised: 7 May 2026
Accepted: 8 May 2026
Published: 9 May 2026

**Copyright:** © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

## 1. Introduction

The rapid digitalization of economic and social life has significantly reshaped patterns of criminality, leading to a pronounced increase in cybercrime worldwide. Computer fraud, including phishing, identity theft, and online financial scams, has become especially widespread and damaging [1–3]. The proliferation of digital infrastructure in banking, commerce, and daily interactions has exponentially expanded criminal opportunities while simultaneously increasing the risk exposure of individuals, businesses, and public institutions [4,5]. While the precise scale of cyber-enabled fraud is difficult to measure due to underreporting, available data suggests a persistent mismatch between victimization experiences and official crime statistics. Reporting gaps are driven by factors such as lack of awareness, perceived futility of reporting, or reputational concerns among institutions [2,6]. Consequently, public data may reflect only a partial view of this rapidly evolving phenomenon. Several initiatives have been developed at the European level to strengthen

resilience against cyber-enabled crime. Directive 2013/40/EU [7] on attacks against information systems, transposed into Spanish law by Organic Law 1/2015, reinforced the criminalization of digital fraud and related offenses (BOE, 2015) [8]. Europol's Internet Organized Crime Threat Assessment (IOCTA) [9] reports have further highlighted computer fraud as one of the fastest-growing cybercrime phenomena, with significant social and economic implications across Member States [10]. Many studies have focused on specific modalities, such as investment scams or romance fraud, while neglecting a comprehensive structural perspective that integrates regional and demographic variables [5,11–13]. Beyond aggregating individual offenses, computer fraud should be understood as an emergent outcome of a socio-technical system. This system integrates digital connectivity, online financial services, internet use intensity, economic inequalities, criminal opportunities, reporting practices, and institutional capacity for response. From this perspective, regional differences are not merely variations in recorded incidence but expressions of distinct territorial system configurations that condition exposure, detection, and vulnerability. From a theoretical perspective, this approach aligns with Routine Activity Theory, which emphasizes exposure and opportunity structures, and with the Technology Acceptance Model (TAM), which explains how the expansion of digital environments increases both adoption and vulnerability. Together, these frameworks support the interpretation of computer fraud as an emergent outcome of interactions between users, technologies, and institutional contexts. Within this framework, the system comprises three components (digital, socioeconomic, and territorial) that interact to shape exposure to online environments and the incidence of computer fraud. Accordingly, higher levels of digital integration and economic activity are expected to increase fraud exposure, while territorial differences modulate these patterns through institutional and reporting factors. However, there is still a lack of studies that examine computer fraud as a multiscale systemic phenomenon and analyze how interdependent digital, socioeconomic, and territorial components generate differentiated patterns of vulnerability across regions. To design effective, evidence-based prevention strategies, it is therefore essential to understand how these interconnected factors shape the spatial and temporal dynamics of computer fraud. Vulnerability to computer fraud arises from the interaction between digital infrastructures, socioeconomic conditions, and territorial contexts. Greater digital connectivity increases exposure to online fraud, while economic development expands participation in digital financial systems. Territorial differences in institutional capacity and technological adoption further shape the regional distribution of fraud. Thus, vulnerability patterns reflect interconnected components of the system rather than isolated factors. Existing research on computer fraud can be broadly grouped into three strands: studies focusing on specific fraud modalities, analyses of individual risk factors, and research examining the role of digitalization and socioeconomic development. However, these approaches often remain fragmented and rarely integrate structural, territorial, and temporal dimensions. Despite extensive research on cyber fraud, most studies focus on specific modalities or isolated risk factors, often neglecting the interaction between digital, socioeconomic, and territorial dimensions. Few adopt an integrated approach combining temporal, regional, and structural analyses.

This study addresses this gap by adopting a socio-technical systems perspective that integrates temporal dynamics, regional disparities, and structural determinants within a unified analytical framework. Unlike previous studies that focus on isolated factors or specific fraud types, this approach provides a multiscalar analysis of computer fraud in Spain, including trends, regional clustering, structural associations, and medium-term projections to 2035. Spain represents a relevant case for analyzing computer fraud due to its rapid digitalization, pronounced regional heterogeneity, and decentralized structure, which enable the study of differentiated vulnerability patterns within a common national context.

The availability of consistent long-term data further supports the analysis of temporal and regional dynamics. Guided by this framework, the study tests the following hypotheses. Higher levels of digital integration are expected to increase the incidence of fraud due to greater exposure to online environments. Socioeconomic development is also expected to be positively associated with fraud rates, reflecting greater participation in digital economic activity. In addition, territorial differences are expected to produce heterogeneous patterns of fraud, shaped by variations in institutional capacity and reporting practices. Finally, computer fraud is expected to show sustained temporal growth over the study period.

This study approaches computer fraud as a socio-technical and territorial system. Accordingly, the aim was to examine the temporal evolution and regional disparities of different subtypes of computer fraud in Spain from 2011 to 2022, analyze their sociodemographic and structural determinants, identify clustered territorial trajectories across autonomous communities, and provide medium-term projections to 2035 to inform evidence-based public policy and strategic economic planning in the field of digital security. From a systems perspective, computer fraud can be understood as an emergent phenomenon arising from the interactions among multiple interconnected components rather than from isolated causal factors. This view is consistent with systems and complexity approaches, which emphasize interdependencies, non-linear dynamics, and the role of structural configurations in shaping outcomes. Compared to traditional criminological models focused on individual risk factors, the socio-technical framework adopted here highlights how digital infrastructures, user behavior, and institutional contexts interact to generate differentiated patterns of vulnerability and growth.

This study is organized as follows. Section 2 describes the data sources and methods, Section 3 presents the results, and Section 4 discusses the findings from a socio-technical systems perspective. Finally, Section 5 summarizes the main conclusions and implications.

## 2. Methods

### *2.1. Conceptual Systems Framework*

This study examines computer fraud as a socio-technical and territorial system in which fraud incidence emerges from the interaction between digital infrastructures, financial service use, intensity of online activity, socioeconomic conditions, territorial exposure, and institutional reporting practices. Within this framework, Spain's autonomous communities are treated as territorial subsystems embedded in a broader national digital environment. The analytical design distinguishes between structural components of the system (income, education, digital access, and internet use), system states and outputs (incidence rates of total computer fraud and its subtypes), territorial differentiation (regional variation and clustering), and temporal dynamics (trend analysis and projections). K-means clustering was applied as an exploratory method to identify general patterns of regional differentiation. Linear regression models were used as a first-order approximation to capture overall temporal trends and to generate interpretable medium-term projections. Given the relatively limited time series and the exploratory nature of the analysis, linear models provide a robust and transparent baseline for identifying general growth patterns. However, they do not capture potential non-linear dynamics or structural breaks. The projections assume continuity of the observed trends over time and do not incorporate potential changes in policy, technological innovation, or user behavior. Therefore, they should be interpreted as exploratory estimates of possible future trajectories rather than precise predictions. This system-level approach enables assessment of how interconnected digital, economic, and territorial conditions shape heterogeneous patterns of fraud exposure across regions and over time. Within this framework, Spain's 17 autonomous communities and two autonomous cities are considered territorial subsystems embedded within the national

socio-technical environment, allowing the analysis of spatial heterogeneity in fraud incidence under a common regulatory context. To ensure comparability, annual fraud rates were calculated per 100,000 inhabitants using mid-year population data from the National Statistics Institute (INE) [14].

### 2.2. Data Source and Case Definitions

The study used data from the Spanish Ministry of the Interior's Statistical Crime Portal (PEC), including officially recorded cases of computer fraud in Spain between 2011 and 2022. The series begins in 2011 to ensure comparability under consistent national reporting criteria. These statistics are compiled annually by municipal, regional, and national law enforcement agencies. It should be noted that older data from Catalonia and the Basque Country may be incomplete because the Mossos d'Esquadra and the Ertzaintza were incorporated into the national reporting system later. Annual population data from the National Statistics Institute (INE) were used to calculate incidence rates per 100,000 inhabitants. In line with the system-level analytical approach adopted here, the reported fraud data were examined alongside structural variables representing key components of the socio-technical environment in which fraud risk emerges.

Utilizing data from the National Institute of Statistics (INE), which breaks down the population of 16 and older by autonomous community [15]. Illiteracy and complete/incomplete elementary education, complete/incomplete secondary education, vocational training, and higher education were among the seven categories. Based on the INE's Atlas of Household Income Distribution classifications, income level was also included [16]. The national median annual net income of €18,316 in 2022 determines these categories. Four groups were identified: low income (less than €13,737), lower-middle income (€13,737–€18,316), upper-middle income (€18,316–€36,632), and high income (above €36,632). To account for digital behavior patterns, we also included data on Internet and social media use among the population aged 16 to 74. These data were drawn from the INE's ICT Survey on Households for 2022 [17]. Two complementary indicators were analyzed: daily internet use (access on five or more days per week) and multiple daily internet use (several connections per day). Both serve as proxies for the intensity and frequency of online activity across Spain's regions. Lastly, household access to technological equipment was examined using national data from the INE [18]. This included the percentages of homes with a computer, internet access, a broadband connection, a landline, and a mobile phone. Unless otherwise specified, all values refer to the year 2022. These indicators were selected to capture regional variation in the structural configuration of the socio-technical system, including economic resources, educational composition, connectivity, and intensity of digital participation.

### 2.3. Legal and Methodological Criteria for the Classification of Digital Fraud

For this study, computer fraud was classified into four categories according to the official typology of the Spanish Ministry of the Interior, which aligns with the legal framework of the Spanish Criminal Code. This classification distinguishes between bank fraud, credit/debit card and traveler's check fraud, computer scams, and other scams, reflecting different forms of technological mediation, user interaction, and financial exposure. This study classified computer fraud offenses registered under statistical code 2209 of the Spanish Ministry of the Interior into four categories: bank scams, credit/debit card and traveler's check scams, computer scams, and other scams. From a systems perspective, these categories represent different functional expressions of fraud within the broader digital economic environment, each associated with distinct forms of technological mediation, user interaction, and financial exposure. Legally, these forms of fraud are regulated in

Articles 248 to 251 bis of the Spanish Criminal Code (Ley Orgánica 10/1995) [19], which define the general offense of fraud and its aggravated forms, article 623.4, applicable before the 2015 reform, covered low-value fraud as a misdemeanor. The reform introduced by Organic Law 1/2015 (BOE-A-2015-3439) [8] updated thresholds for criminal liability and explicitly addressed technology-based fraud. Computer fraud corresponds to Article 249.1. a (previously 248.2.a), which penalizes obtaining financial gain through computer manipulation or similar deceit. It is considered a cyber-dependent crime that requires digital means and includes schemes such as malware attacks, spoofing, and system simulation [20]. Bank fraud, while legally part of general fraud provisions, was treated separately due to its link to online banking and payment platforms, involving phishing, identity theft, and unauthorized access. From a socio-technical systems perspective, this subtype can be understood as a component of the digital financial subsystem, shaped by the interactions among banking infrastructures, remote authentication practices, payment technologies, and offender adaptation strategies. Fraud with credit/debit cards and traveler's checks includes unauthorized use, cloning, and theft-related fraud. The category "other scams" includes fraud types that do not fit into the previous categories, such as fraudulent online advertisements, deceptive sales, or informal phishing schemes.

### *2.4. Temporal Trend Analysis (2011–2022) and Predictive Modeling to 2035*

Linear regression models were fitted to annual fraud-rate data to estimate the direction and magnitude of change over time at the national and regional levels. Within the system-level framework adopted here, these models were used to characterize the temporal dynamics of the fraud system and its territorial evolution. The slope of the regression line indicated the annual growth rate, and the coefficient of determination ($R^2$) assessed model fit. All models assumed linearity. The statistical significance of each regression slope was assessed using a *t*-test, and the corresponding *p*-values are reported. Based on the regression coefficients, forward projections were generated to estimate fraud incidence through 2035. These forecasts were computed assuming that past linear trends would persist and that no major policy, technological, or societal disruptions would substantially alter the current trajectory of the system.

### *2.5. Cluster Analysis of Computer Fraud Rates Across Spanish Regions*

A cluster analysis was performed using the K-means algorithm to classify the autonomous communities according to their mean computer fraud rates between 2011 and 2022 [21]. In the present study, clustering was used to identify regional system profiles, that is, recurrent territorial configurations with similar levels of fraud exposure. The dataset consisted of standardized annual fraud rates per 100,000 inhabitants. The optimal number of clusters was determined using the Elbow method [22]. We tested k = 2–6; the solution with k = 5 explained over 70% of the total variance and represented the best trade-off between within-cluster homogeneity and between-cluster separation. Cluster robustness was evaluated using silhouette scores (all > 0.6), confirming the classification's adequacy. The K-means algorithm was then applied to group the Spanish regions into five categories according to their similarity in fraud incidence.

### *2.6. Sex- and Age-Specific Analyses*

To examine differences in computer fraud victimization by sex and age, annual rates were calculated per 100,000 inhabitants using disaggregated population data from the National Statistics Institute (INE). Rates were stratified by sex and grouped into six age categories: under 18, 18–25, 26–40, 41–50, 51–65, and 65 or older. These subgroup analyses were included to capture internal differentiation within the fraud system and to assess whether temporal trajectories varied across demographic segments. Linear regression

models were fitted to estimate temporal trends within each subgroup, and comparisons between male and female trajectories were conducted descriptively. Forecasts by age and sex were derived from these subgroup-specific models.

### *2.7. Statistical Analysis*

All analyses were conducted using SPSS version 29.0 (IBM Corp., Armonk, NY, USA), Excel 2021, and GraphPad Prism 10.0. Results were expressed as absolute frequencies, percentages, means, standard deviations, and incidence rates per 100,000 inhabitants. Temporal trends were assessed using linear regression models. Regional differences in computer fraud rates were examined using a Type II ANOVA on regression models that included the Year × Region interaction. To identify spatial inequalities in computer fraud incidence, mean annual fraud rates (2011–2022) were computed for each region and compared with the national mean. Measures of dispersion, such as standard deviation and coefficient of variation, were calculated to quantify intra-regional variability over time. Correlation analyses between structural variables representing system-level components (education, income, digital access, and internet use) and offense rates were performed using Pearson or Spearman coefficients, depending on the distribution of the variables. In this way, the statistical analysis combined temporal, territorial, demographic, and structural dimensions to characterize computer fraud as a multicomponent socio-technical phenomenon. Statistical significance was set at $p < 0.05$.

## 3. Results

### *3.1. Cybercrime Patterns in Spain (2011–2022)*

As shown in Figure 1, the mean annual rate per 100,000 inhabitants of the main types of cybercrime recorded in Spain between 2011 and 2022. The data show that computer fraud was the most frequent cyber offense, with a mean rate of 269.4 cases, clearly surpassing all other categories. The second most reported category was threats and coercion, with a mean of 25.7 cases, followed by computer forgery (9.4) and illegal access and interception, which registered a mean of 6.9 cases per 100,000 inhabitants during the same period. Other categories reported lower mean rates: offenses against persons (3.6), sexual offenses committed through digital means (2.8), and data and system interference (2.3). The lowest rate was observed in industrial and intellectual property offenses, with a mean of 0.3 cases per 100,000 inhabitants.

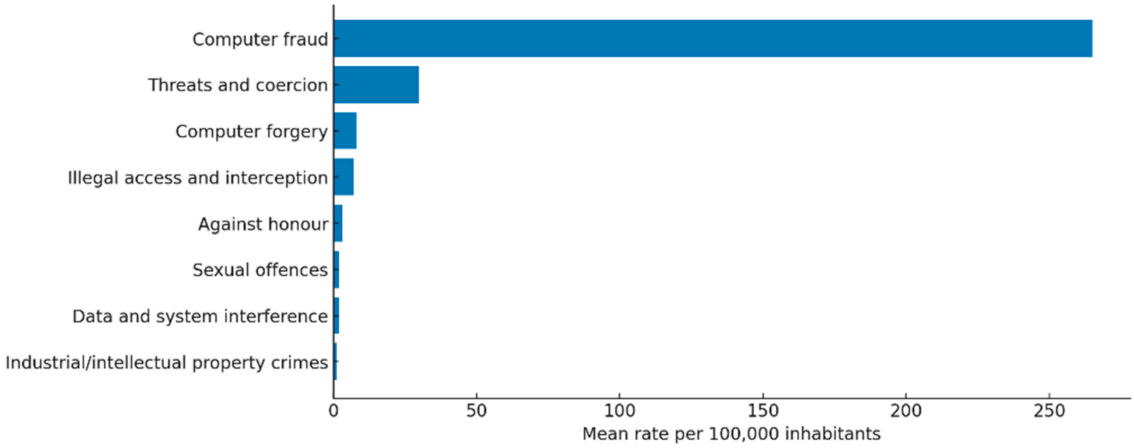



**Figure 1.** Mean annual cybercrime rates in Spain (2011–2022). The figure shows the mean annual rate per 100,000 inhabitants of different types of cybercrime recorded in Spain between 2011 and 2022.

### *3.2. Trends in Computer Fraud in Spain (2011–2022)*

The analysis of the annual evolution of cyber fraud in Spain between 2011 and 2022 showed a very marked and sustained increase (Figure 2A). The rate rose from 44.7 cases per 100,000 inhabitants in 2011 to 133.1 in 2015, then to 292.5 in 2018. The growth intensified in recent years, reaching 409.1 in 2019, 543.5 in 2020, and 707.7 in 2022, representing an increase of over 1.480% over the period analyzed. The regression line (y = 61.12x − 122,976.13) confirmed a steep upward trend, with a mean annual increase of approximately 61 cases per 100,000 inhabitants. As shown in Figure 2B, computer fraud in Spain increased from 44.7 to 707.7 cases per 100,000 inhabitants between 2011 and 2022. The rate is projected to reach about 820 in 2025, 1100 in 2030, and nearly 1440 in 2035.

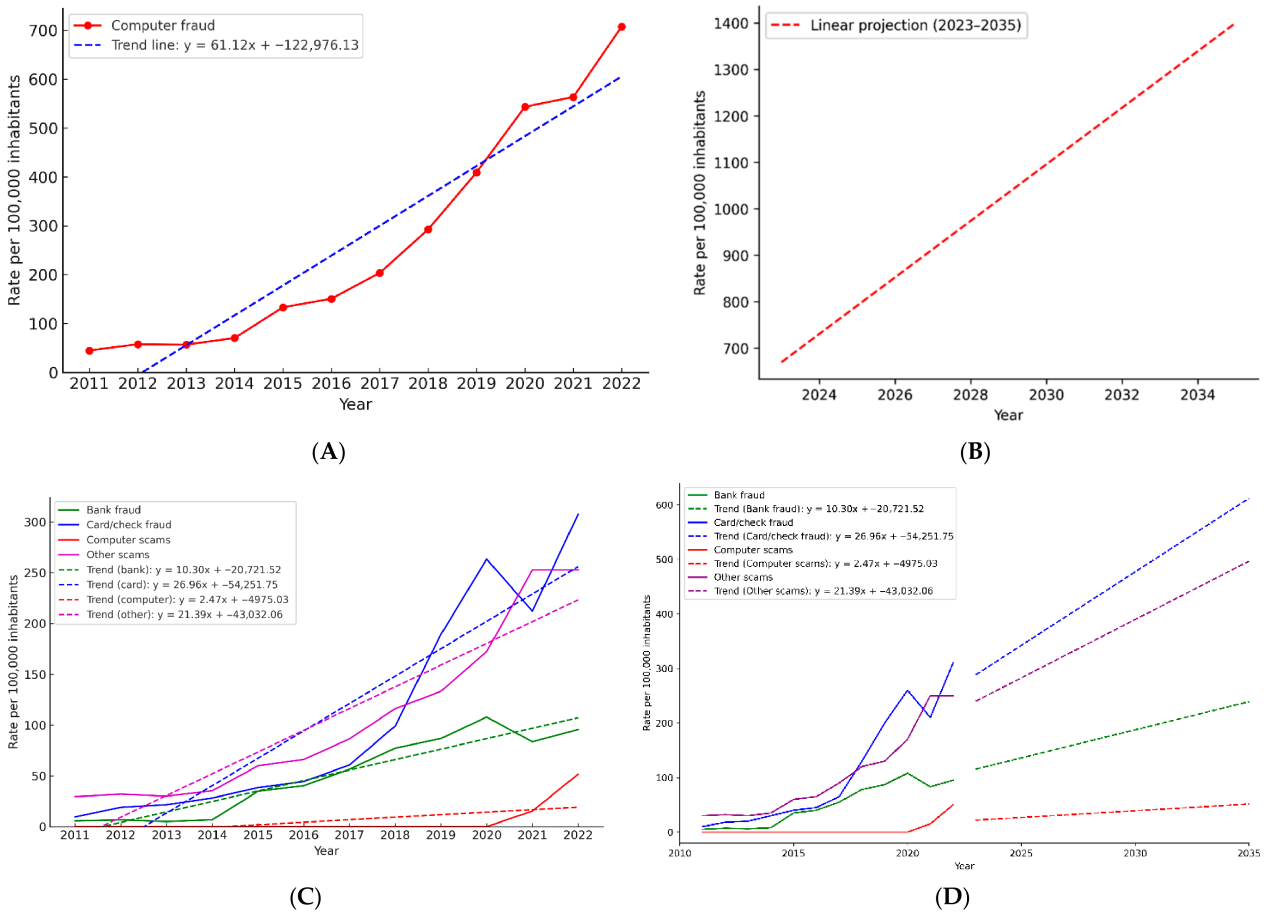



**Figure 2.** Evolution and trends in different forms of computer fraud in Spain (2011–2022). (**A**) Annual evolution and linear trend of total computer fraud in Spain. It shows the annual rate of computer fraud offenses recorded between 2011 and 2022 per 100,000 inhabitants. A linear trend line (y = 61.12x − 122,976.13) highlights the steady, accelerating growth of this cybercrime category. (**B**) Linear projection of computer scam rates in Spain (2023–2035). (**C**) Trends in different subtypes of computer fraud. Four subtypes are presented: bank fraud, credit/debit card and traveler's check fraud, computer scams, and other scams. Each series includes a linear trend line illustrating its growth pattern over the study period. (**D**) Projected evolution of computer fraud by subtype in Spain (2023–2035).

The differentiated trajectories of these fraud subtypes reflect the internal evolution of the broader fraud system, with distinct forms of digital and financial exposure contributing unevenly to overall growth. As shown in Figure 2C, different types of computer fraud in Spain increased steadily between 2011 and 2022, with distinct growth patterns. Card fraud showed the largest rise, increasing from 9.5 to 307.5 cases per 100,000 inhabitants, with a

sharp acceleration after 2016 (44.4) and rapid growth through 2018 (99.1), 2019 (189.1), and 2020 (263.3), peaking in 2022. Bank fraud also increased substantially, from 5.6 in 2011 to a peak of 107.9 in 2020 and remained elevated at 95.6 in 2022 despite a slight decline after 2020. Computer scams emerged more recently, first recorded at 15.3 in 2021 and rising to 51.7 in 2022, indicating a rapid recent expansion. These differentiated trends suggest that fraud subtypes are driven by distinct dynamics, reflecting heterogeneous forms of digital and financial exposure within the broader system. Finally, in Figure 2D, it is observed how all types of cyber fraud in Spain increased between 2011 and 2022 and are projected to continue growing until 2035. Card fraud increased the most, rising from 9.5 to 307.5 cases per 100,000 inhabitants, with a projection exceeding 600 in 2035. Additionally, banking fraud increased from 5.6 in 2011 to 95.6 in 2022 and is expected to reach approximately 240 by 2035. Cyber scams, recorded for the first time in 2021 at 15.3 cases and rising to 51.7 in 2022, also show an upward trend, though at a lower growth rate. The remaining frauds analyzed also showed a sustained increase and could reach 500 by 2035.

### *3.3. Regional Variation and Temporal Trends in Computer Fraud*

The analysis of computer fraud rates across Spain's autonomous communities between 2011 and 2022 showed a widespread, statistically significant increase in all regions (Table 1). The annual slopes were significant in all cases ($p < 0.05$), confirming an upward trend during the study period.

**Table 1.** Annual rates and linear trends of computer fraud across Spanish regions (2011–2022).

| Regions | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | Slope | *p*-Value |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Andalusia | 42.8 | 51.8 | 53.1 | 67.4 | 77.8 | 97.3 | 123.7 | 179.9 | 276.2 | 390.3 | 416.5 | 580.3 | 45.216 | $3.43 \times 10^{-5}$ |
| Aragon | 46.9 | 72.9 | 68.8 | 107.6 | 111.5 | 109.8 | 142.1 | 239.2 | 343.8 | 524.3 | 551.2 | 658.4 | 55.301 | $2.4 \times 10^{-5}$ |
| Asturias | 34.8 | 44.1 | 54.8 | 65.0 | 95.3 | 122.5 | 162.0 | 230.6 | 357.5 | 551.9 | 611.5 | 762.5 | 64.681 | $2.07 \times 10^{-5}$ |
| Balearic Islands | 67.3 | 85.4 | 94.4 | 118.2 | 205.0 | 190.8 | 282.8 | 486.4 | 670.1 | 928.6 | 597.2 | 633.3 | 71.214 | 0.0001 |
| Canary Islands | 65.1 | 100.0 | 54.8 | 65.1 | 87.5 | 80.7 | 103.0 | 145.6 | 338.4 | 581.0 | 410.3 | 537.2 | 46.267 | 0.0005 |
| Cantabria | 38.9 | 39.2 | 47.5 | 100.1 | 132.6 | 176.6 | 244.5 | 293.7 | 303.9 | 431.1 | 554.8 | 742.9 | 58.181 | $4.26 \times 10^{-6}$ |
| Castile and Leon | 33.2 | 46.0 | 55.7 | 75.1 | 97.5 | 137.7 | 189.9 | 270.3 | 394.4 | 577.9 | 606.6 | 799.4 | 67.469 | $9.38 \times 10^{-6}$ |
| Castile-La Mancha | 40.7 | 51.5 | 59.7 | 72.6 | 97.7 | 101.6 | 137.6 | 236.3 | 317.0 | 411.0 | 478.0 | 662.7 | 51.795 | $2.13 \times 10^{-5}$ |
| Catalonia | 6.5 | 7.7 | 7.7 | 7.9 | 210.3 | 240.3 | 351.7 | 484.3 | 521.4 | 603.8 | 609.5 | 790.6 | 75.926 | $4.81 \times 10^{-8}$ |
| Valencian Community | 47.9 | 62.3 | 61.3 | 77.9 | 100.5 | 125.9 | 161.7 | 227.3 | 314.9 | 433.4 | 482.9 | 569.6 | 48.007 | $5.15 \times 10^{-6}$ |
| Extremadura | 25.9 | 36.1 | 29.9 | 47.0 | 55.1 | 78.3 | 95.5 | 175.1 | 225.7 | 368.1 | 433.6 | 623.5 | 48.214 | $8.9 \times 10^{-5}$ |
| Galicia | 38.3 | 52.3 | 54.9 | 68.5 | 96.2 | 112.9 | 163.5 | 253.0 | 370.4 | 469.9 | 723.2 | 686.0 | 63.281 | $2.7 \times 10^{-5}$ |
| Madrid | 56.5 | 74.3 | 71.2 | 79.4 | 108.8 | 111.5 | 136.6 | 251.0 | 492.9 | 651.0 | 695.8 | 856.2 | 73.315 | $5.23 \times 10^{-5}$ |
| Murcia | 20.8 | 32.7 | 29.1 | 39.6 | 48.9 | 60.4 | 80.5 | 137.6 | 224.8 | 389.5 | 444.8 | 564.7 | 46.947 | $9.62 \times 10^{-5}$ |
| Navarre | 48.3 | 79.4 | 95.0 | 123.6 | 200.6 | 222.3 | 268.6 | 328.3 | 417.9 | 590.3 | 555.2 | 725.2 | 59.777 | $3.02 \times 10^{-7}$ |
| Basque Country | 6.5 | 9.4 | 8.9 | 7.4 | 280.1 | 317.6 | 389.5 | 552.5 | 624.7 | 747.2 | 678.2 | 854.1 | 85.617 | $8.95 \times 10^{-8}$ |
| Rioja | 19.8 | 38.0 | 37.9 | 41.7 | 50.1 | 45.0 | 53.3 | 213.8 | 314.4 | 558.6 | 561.0 | 672.7 | 60.828 | 0.000112 |
| Ceuta | 76.5 | 78.6 | 38.0 | 75.3 | 73.6 | 75.7 | 84.7 | 213.8 | 382.2 | 426.4 | 481.3 | 564.3 | 47.808 | $9.54 \times 10^{-5}$ |
| Melilla | 28.0 | 14.9 | 23.9 | 43.8 | 35.1 | 33.7 | 37.2 | 203.7 | 278.7 | 403.1 | 403.4 | 386.3 | 41.175 | $8.39 \times 10^{-5}$ |

Rates were expressed per 100,000 inhabitants. Regions correspond to Spain's autonomous communities. The table shows the annual rate of computer fraud from 2011 to 2022, the estimated annual increase (slope), the associated *p*-value, and the statistical significance of the linear trend in each region based on simple linear regression. The *p*-value corresponds to a *t*-test assessing whether the slope differs significantly from zero. A *p*-value < 0.05 was considered statistically significant.

The steepest increases were observed in the Basque Country, Catalonia, and Madrid, with annual slopes of 85.6, 75.9, and 73.3 cases per 100,000 inhabitants, respectively. Other regions, including the Balearic Islands, Castile and León, Asturias, Galicia, La Rioja, Navarre, Cantabria, and Aragon, also showed marked increases, whereas Castilla-La Mancha, the Canary Islands, Murcia, Andalusia, the Valencian Community, Extremadura, Ceuta, and Melilla presented moderate but still statistically significant growth. Overall, the regional trajectories indicate a generalized increase in computer fraud, but at different rates across territories.

The linear regression model (Rate per Year × Region) confirmed significant differences between autonomous communities ($p < 0.00000001$), a strong temporal effect ($p < 2.88 \times 10^{-79}$), and a significant year × region interaction ($p = 0.0015$), indicating that, although the increase was widespread, the rate of growth of cyber fraud varied significantly between autonomous communities.

### *3.4. Mean Computer Fraud Rates by Region (2011–2022)*

The analysis of mean computer fraud rates in Spanish autonomous communities from 2011 to 2022 revealed substantial regional disparities (Figure 3). As illustrated in Figures 3 and 4, this spatial distribution reveals a clear concentration of higher rates in economically developed and highly digitalized regions. These territorial differences indicate that computer fraud does not expand uniformly across Spain, but reflects variations in digital integration, economic activity, and institutional capacity across regions. The Basque Country recorded the highest mean rate, with 373.0 cases per 100,000 inhabitants, closely followed by the Balearic Islands at 363.3 and Catalonia at 320.1. These three regions constituted the first group in terms of prevalence, standing notably above the national means. In the second, Navarre (304.6), Madrid (298.8), and Castile and León (273.6) also showed elevated mean rates, suggesting persistently high levels of computer fraud throughout the study period. Cantabria, Asturias, and Galicia presented nearly identical means, around 258 cases per 100,000 inhabitants. A mid-range group included Aragon (248.0), Castile-La Mancha (222.2), the Valencian Community (222.1), along with La Rioja (217.2), Ceuta (214.2), and the Canary Islands (214.01). These regions exhibited moderate mean rates, indicating the presence of computer fraud, though on a less pronounced scale than in the territories mentioned above. At the lower end of the distribution, Andalusia (196.4), Extremadura (182.8), and Murcia (172.8) registered relatively modest mean rates. The lowest mean was recorded in Melilla, with 157.7 cases per 100,000 inhabitants, making it the region least exposed to computer fraud during the study period.

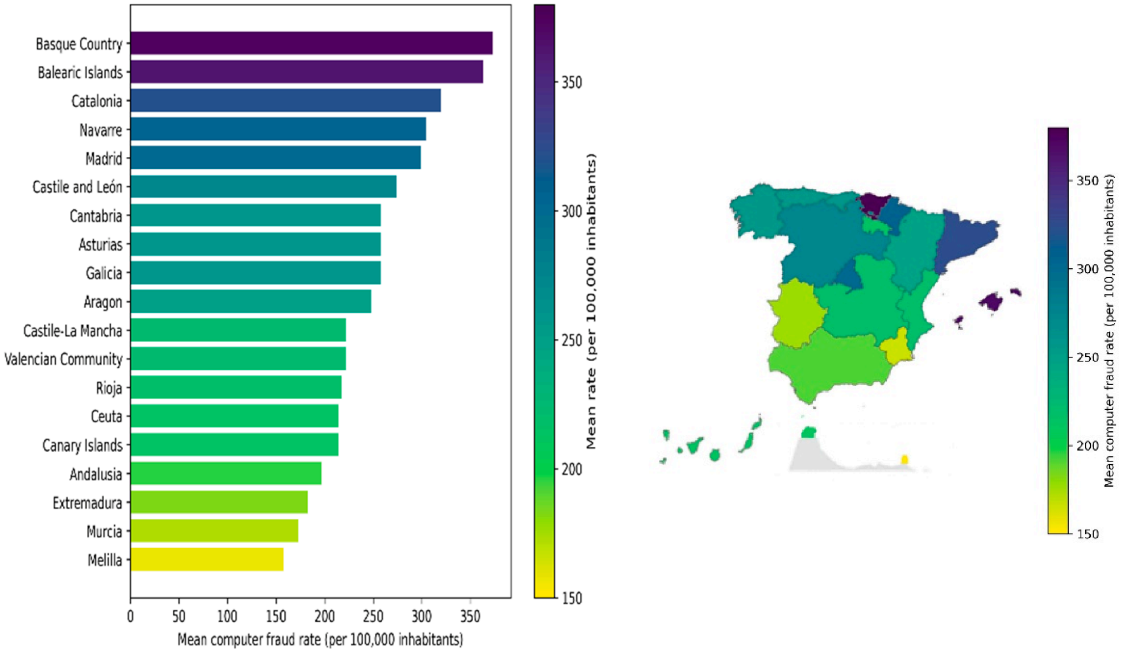



**Figure 3.** Mean computer fraud rate by Spanish region (2011–2022). Mean annual rate of computer fraud per 100,000 inhabitants across Spain's autonomous communities, displayed in descending order to facilitate comparison. A consistent color scale (150–380 cases per 100,000 inhabitants) is applied, with darker colors indicating higher incidence rates, ensuring visual comparability with the geographic representation. From 2011 to 2014, data included reports from the National Police, Civil

Guard, Navarre's Foral Police, and local police forces contributing to the Criminal Statistics System. From 2015 onward, data from the Mossos d'Esquadra are included, and from 2021 onward, data from the Ertzaintza are incorporated.

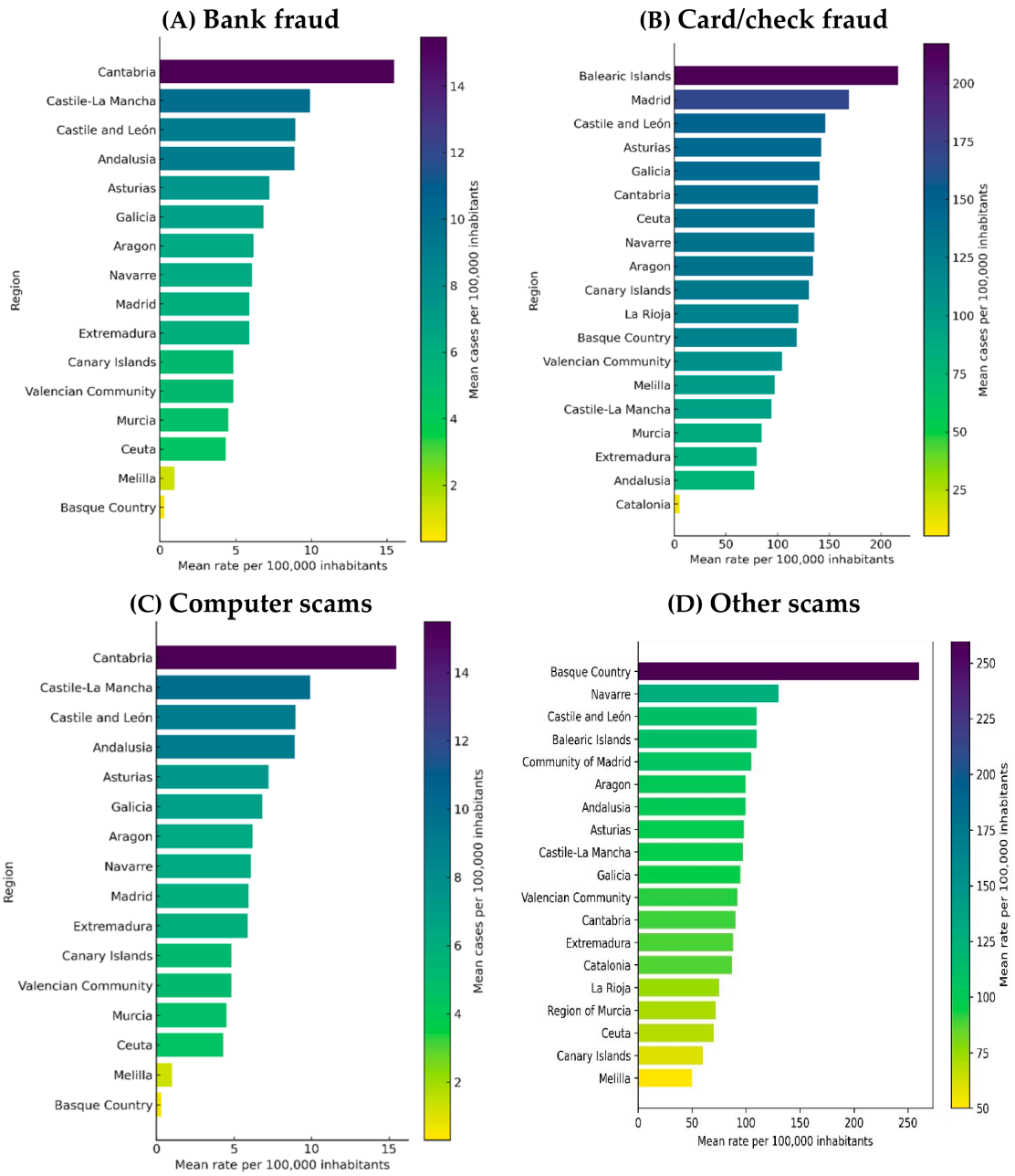



**Figure 4.** Regional distribution of computer fraud types in Spain: mean rates by autonomous community (2011–2022). Mean annual rates per 100,000 inhabitants are shown for four fraud categories: (**A**) bank fraud, (**B**) credit/debit card and traveler's check fraud, (**C**) computer scams, and (**D**) other scams. A consistent color scale is applied across panels, with darker colors indicating higher incidence rates, facilitating comparison between regions and fraud types. From 2011 to 2014, data included reports from the National Police, Civil Guard, Navarre's Foral Police, and local police forces contributing to the Criminal Statistics System. From 2015 onward, data from the Mossos d'Esquadra are included, and from 2021 onward, data from the Ertzaintza are incorporated.

### *3.5. Regional Distribution of Fraud Types in Spain*

The analysis of regional fraud rates in Spain reveals distinct geographical patterns across the four main types, measured per 100,000 inhabitants, from 2011 to 2022 (Figure 4). The annual mean rate of bank fraud per 100,000 inhabitants in Spain between 2011 and 2022

varied notably across regions (Figure 4A). Catalonia recorded the highest mean rate, with 227.42 cases, well above the rest. This figure may be upwardly biased due to differences in the classification of offenses included in this subtype across autonomous communities. The Balearic Islands followed with a mean rate of 37.90 cases, while Navarre (32.40), Castilla-La Mancha (21.79), the Valencian Community (21.07), Madrid (20.88), and the Canary Islands (19.37) also registered relatively high mean rates. In Figure 4B, which shows fraud involving credit/debit cards and traveler's checks, the Balearic Islands ranked first (217.1). Madrid (168.8) also recorded high levels. At the lower end, Extremadura (79.6), Andalusia (77.4), and Catalonia (5.1) were below the national mean. The Catalonia figure may be downwardly biased due to differences in the classification of offenses included in this subtype compared with other autonomous communities. Figure 4C shows computer fraud. Cantabria ranked first (15.5), followed by Castile-La Mancha (9.9) and Castile and León (9.0). The lowest rates were found in Catalonia and the Basque Country, below 1.

Lastly, Figure 4D highlights other types of fraud, showing a markedly different profile: the Basque Country reports an exceptionally high mean rate (253.3), more than twice that of the next highest region, Navarre (130.7). Castilla y León, the Balearic Islands, and Madrid follow with values just above 100, while Melilla (50.7), the Canary Islands (59.8), and Ceuta (70.0) remain at the lower end of the scale.

### *3.6. Regional System Profiles and Clustering of Fraud Rates*

Five clusters of Spanish regions were identified using K-means clustering of mean fraud rates per 100,000 inhabitants from 2011 to 2022, revealing distinct regional system profiles of fraud exposure. The composition of the clusters was summarized in Table 2, which lists all regions and their corresponding mean rates. These clusters can be interpreted as recurrent territorial configurations of the fraud system, reflecting different levels of structural exposure and digital vulnerability. Cluster 0 comprises Extremadura, the Region of Murcia, and Melilla, with the lowest national means (171.1). Cluster 1 includes Castile-La Mancha, the Valencian Community, La Rioja, Ceuta, the Canary Islands, and Andalusia, with a mean rate of 214.4. Cluster 2 brings together Castile and León, Cantabria, Asturias, Galicia, and Aragon, with a mean value of 259.1. Cluster 3 consists of Catalonia, Navarre, and the Community of Madrid, which recorded higher levels (mean: 307.8). Finally, Cluster 4, with the highest means (368.2), groups the Basque Country and the Balearic Islands. The groups were renumbered from 0 to 4 in ascending order according to their mean fraud rates. The values reported represent the mean number of computer fraud cases per 100,000 inhabitants between 2011 and 2022.

**Table 2.** Mean computer fraud rates per 100,000 inhabitants (2011–2022) and Spanish regions included in each cluster.

| Clusters | Mean Rate (2011–2022) | Regions |
|---|---|---|
| Cluster 0 | 171.1 | Extremadura, Murcia, Melilla |
| Cluster 1 | 214.4 | Andalusia, Canary Islands, Castilla-La Mancha, Ceuta, Rioja, Valencian Community |
| Cluster 2 | 259.1 | Castile and León, Cantabria, Asturias, Galicia, Aragón |
| Cluster 3 | 307.8 | Catalonia, Navarre, Madrid |
| Cluster 4 | 368.2 | Balearic Islands, Basque Country |

Clusters were renumbered from 0 to 4 in ascending order of mean fraud rates. The values represent the mean number of reported computer fraud cases per 100,000 inhabitants from 2011 to 2022.

### *3.7. Cluster Analysis of Regional Fraud Rates*

Figure 5 displays the temporal trends of the five clusters, ordered from the lowest to the highest mean rate, to provide a clearer picture of the dynamics within each group. It also highlights the grouping of regions into distinct clusters, reflecting different temporal

trajectories and levels of fraud exposure across the national system. Cluster 0 (Figure 5A) consists of Melilla, the Region of Murcia, and Extremadura. These regions recorded the lowest national means, ranging from 157.6 in Melilla to 182.8 in Extremadura. All three showed moderate growth until 2017, followed by a sharper increase that continued through the end of the period. In 2022, their rates ranged between 386 and 624 incidents per 100,000 inhabitants. Cluster 1 (Figure 5B) brings together Andalusia, the Canary Islands, Ceuta, La Rioja, the Valencian Community, and Castile-La Mancha. Their mean values ranged from 196.4 (Andalusia) to 222.2 (Castile-La Mancha). Starting at around 20–75 incidents in 2011, all regions experienced sharp increases after 2017, ending in 2022 at 537–673. Castile-La Mancha and La Rioja showed the highest rates at the end of the series. Cluster 2 (Figure 5C) includes Aragon, Galicia, Asturias, Cantabria, Castile, and León. The mean values of this group ranged from 248.0 in Aragon to 273.6 in Castile and León. Initial rates in 2011 ranged from 33 to 47, and by 2022, they had increased substantially, reaching between 658 and over 799. Cantabria and Galicia were among the regions with the steepest increases in recent years. Cluster 3 (Figure 5D) comprises the Community of Madrid, Navarre, and Catalonia. These three regions showed higher mean levels: Catalonia at 320.1, Navarre at 304.6, and Madrid at 298.8. Their trajectories revealed steady growth throughout the period, culminating in 2022 with high values of 725.2 in Navarre, 790.6 in Catalonia, and 856.2 in Madrid. Finally, Cluster 4 (Figure 5E) includes the Balearic Islands and the Basque Country, which consistently displayed the highest national means. The Basque Country recorded the highest means (373.0), followed by the Balearic Islands (363.3). Their trajectories were marked by strong growth between 2015 and 2020, with the Balearic Islands peaking at more than 925 incidents per 100,000 inhabitants before slightly declining, while the Basque Country remained above 850 in the last year.

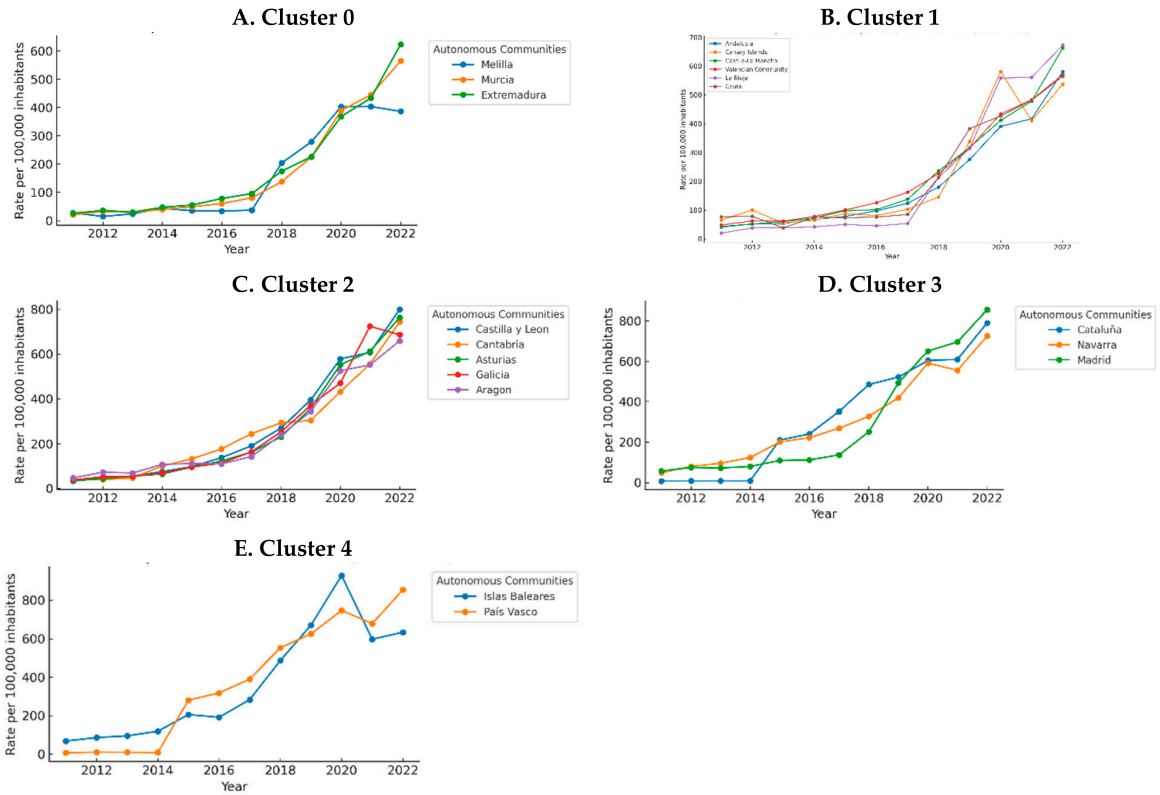



**Figure 5.** Cluster analysis of computer fraud rates by autonomous community in Spain (2011–2022). Each panel shows the communities grouped by their mean computer fraud incidence rate per 100,000 inhabitants during the study period. This classification identifies regional system profiles and highlights territorial differences in the structural configuration of fraud exposure.

### *3.8. System-Level Determinants of Computer Fraud (2022)*

Table 3 shows statistically significant system-level associations between various sociodemographic, educational, economic, and technological variables and the rates of computer fraud recorded in Spain in 2022. These associations help characterize the structural configuration of the socio-technical environment in which fraud risk emerges across regions. A significant correlation was found between educational level and the prevalence of other scams in 2022. Specifically, higher education showed a positive correlation with this type of fraud (r = 0.581, $p$ = 0.014), while both intermediate education (r = −0.597, $p$ = 0.011) and the first stage of secondary education (r = −0.607, $p$ = 0.010) were negatively associated. The observed variation in the relationship between education and fraud can be interpreted in terms of differential exposure and participation in digital environments. Higher educational attainment is often associated with greater use of online financial services, digital platforms, and complex economic transactions, which may increase exposure to fraud opportunities. In contrast, individuals with intermediate levels of education may have lower engagement with such systems, thereby reducing their exposure. These patterns suggest that education does not act as a simple protective factor, but rather interacts with digital behavior and economic activity, shaping distinct vulnerability profiles within the broader socio-technical system. No other significant correlations were observed between the remaining educational categories and the different types of fraud, including bank fraud, card/check fraud, and computer scams ($p$ > 0.05). On the other hand, a significant correlation was found between income level and the incidence of other scams. Specifically, high income was strongly positively correlated with this type of fraud (r = 0.691, $p$ = 0.001). No other statistically significant associations were observed between income categories and the remaining types of fraud (bank fraud, card/check fraud, and computer scams), although lower-middle income showed a marginally non-significant negative correlation with other scams (r = −0.465, $p$ = 0.052). Taken together, these findings suggest that fraud incidence is shaped not by isolated variables, but by the interaction of multiple structural components of the regional socio-technical system. A significant correlation was observed between frequent Internet usage and certain types of fraud. Specifically, multiple daily uses of the Internet showed a positive correlation with bank fraud (r = 0.281, $p$ = 0.039), a negative correlation with card/check fraud (r = −0.353, $p$ = 0.009), and a negative correlation with computer scams (r = −0.318, $p$ = 0.019). No other significant correlations were found between Internet usage rates and other types of fraud ($p$ > 0.05). Finally, strong correlations were found between digital household equipment and computer-related fraud. Broadband access showed the highest correlation with bank fraud (r = 0.968, $p$ = 0.000) and other scams (r = 0.925, $p$ = 0.000), closely followed by general Internet access and mobile connectivity. In contrast, landline access was negatively associated with all fraud types, most notably with other scams (r = −0.953, $p$ = 0.000) and card/check fraud (r = −0.913, $p$ = 0.000). While positively associated, computer ownership showed a weaker correlation with computer scams (r = 0.552, $p$ = 0.098), which did not reach statistical significance. High digital connectivity, combined with greater economic activity and regional exposure to online transactions, appears to amplify vulnerability patterns across territories.

**Table 3.** Analyze correlations between sociodemographic, educational, economic, and technological variables and the incidence of computer fraud (2022).

| Types of Computer Fraud | Bank Fraud | Card/Check Fraud | Computer Scams | Other Scams |
|---|---|---|---|---|
| A. Educational level | | | | |
| Illiterate | 0.019 ($p$ = 0.941) | −0.464 ($p$ = 0.061) | −0.133 ($p$ = 0.612) | −0.244 ($p$ = 0.346) |
| Intermediate education | −0.143 ($p$ = 0.584) | −0.194 ($p$ = 0.455) | 0.187 ($p$ = 0.472) | −0.597 ($p$ = 0.011) |
| Incomplete Primary Education | −0.047 ($p$ = 0.858) | −0.431 ($p$ = 0.084) | −0.110 ($p$ = 0.673) | −0.083 ($p$ = 0.752) |
| Primary Education | 0.124 ($p$ = 0.634) | −0.175 ($p$ = 0.503) | 0.022 ($p$ = 0.934) | 0.234 ($p$ = 0.366) |
| First stage of Secondary Education | −0.176 ($p$ = 0.499) | −0.071 ($p$ = 0.786) | 0.251 ($p$ = 0.331) | −0.607 ($p$ = 0.010) |
| Second stage of Secondary Education | 0.041 ($p$ = 0.877) | 0.238 ($p$ = 0.358) | −0.133 ($p$ = 0.610) | −0.275 ($p$ = 0.286) |
| Secondary education, vocational training | −0.153 ($p$ = 0.557) | 0.048 ($p$ = 0.853) | 0.200 ($p$ = 0.441) | 0.014 ($p$ = 0.959) |
| Higher education | 0.130 ($p$ = 0.618) | 0.234 ($p$ = 0.367) | −0.162 ($p$ = 0.536) | 0.581 ($p$ = 0.014) |
| B. Mean annual net income per inhabitant | | | | |
| Low | −0.195 ($p$ = 0.437) | −0.209 ($p$ = 0.406) | 0.125 ($p$ = 0.620) | −0.002 ($p$ = 0.994) |
| Lower middle | −0.100 ($p$ = 0.692) | −0.076 ($p$ = 0.765) | −0.017 ($p$ = 0.947) | −0.465 ($p$ = 0.052) |
| Upper middle | 0.096 ($p$ = 0.704) | 0.217 ($p$ = 0.386) | 0.207 ($p$ = 0.409) | −0.283 ($p$ = 0.255) |
| High | 0.225 ($p$ = 0.370) | 0.105 ($p$ = 0.677) | −0.318 ($p$ = 0.198) | 0.691 ($p$ = 0.001) |
| C. Internet and social media usage rate | | | | |
| Ever used the Internet | 0.313 ($p$ = 0.206) | −0.261 ($p$ = 0.295) | −0.310 ($p$ = 0.210) | 0.006 ($p$ = 0.982) |
| Use in the last 12 months | 0.085 ($p$ = 0.622) | −0.081 ($p$ = 0.639) | −0.111 ($p$ = 0.517) | −0.021 ($p$ = 0.904) |
| Use in the last 3 months | 0.068 ($p$ = 0.624) | −0.030 ($p$ = 0.831) | −0.108 ($p$ = 0.436) | 0.017 ($p$ = 0.905) |
| Weekly use | 0.098 ($p$ = 0.481) | −0.081 ($p$ = 0.563) | −0.109 ($p$ = 0.435) | −0.031 ($p$ = 0.826) |
| Daily use | 0.097 ($p$ = 0.485) | −0.171 ($p$ = 0.215) | −0.115 ($p$ = 0.407) | −0.102 ($p$ = 0.462) |
| Multiple daily uses | 0.281 ($p$ = 0.039) | −0.353 ($p$ = 0.009) | −0.318 ($p$ = 0.019) | 0.000 ($p$ = 1.000) |
| D. Type of Internet access equipment and computer connections | | | | |
| Computer | 0.936 ($p$ = 0.000) | 0.897 ($p$ = 0.000) | 0.552 ($p$ = 0.098) | 0.952 ($p$ = 0.000) |
| Internet Access | 0.966 ($p$ = 0.000) | 0.919 ($p$ = 0.000) | 0.515 ($p$ = 0.127) | 0.923 ($p$ = 0.000) |
| Broadband | 0.968 ($p$ = 0.000) | 0.920 ($p$ = 0.000) | 0.516 ($p$ = 0.126) | 0.925 ($p$ = 0.000) |
| Landline | −0.715 ($p$ = 0.020) | **−0.913 ($p$ = 0.000)** | **−0.865 ($p$ = 0.001)** | −0.953 ($p$ = 0.000) |
| Mobile | 0.947 ($p$ = 0.000) | 0.958 ($p$ = 0.000) | 0.553 ($p$ = 0.097) | 0.952 ($p$ = 0.000) |

Values represent Pearson correlation coefficients (r) and $p$-values between variables related to internet use, educational attainment, and technological access, as well as the rates of computer fraud per 100,000 inhabitants. Statistical significance ($p < 0.05$) is highlighted.

### *3.9. Sex and Age Differences in Computer Fraud Rates*

Comparative analysis of fraud victimization rates by sex, age group, and fraud type in Spain between 2011 and 2022 reveals consistent patterns across all demographic segments. However, no statistically significant differences by sex were found (Table 4). Focusing on the most common type, card and check fraud, among those under 18, both sexes showed very low mean rates (0.69 for men versus 0.75 for women; t = −0.003, $p$ = 0.998). This trend of low victimization extended to all types of fraud in this age group, and none of the comparisons yielded significant differences.

**Table 4.** Sex-based differences in computer fraud victimization rates across age groups in Spain (2011–2022).

| Fraud Types | Age Groups | Mean (Men) | Mean (Women) | t | *p*-Value |
|---|---|---|---|---|---|
| Bank fraud | Under 18 | 1.0 | 1.044 | −0.098 | 0.923 |
| | 18–25 | 55.228 | 62.694 | −0.358 | 0.724 |
| | 26–40 | 55.425 | 57.722 | −0.123 | 0.903 |
| | 41–50 | 53.259 | 54.283 | −0.057 | 0.955 |
| | 51–65 | 46.27 | 38.312 | 0.525 | 0.605 |
| | Over 65 | 27.003 | 12.985 | 1.597 | 0.129 |
| Card/check fraud | Under 18 | 0.746 | 0.747 | −0.003 | 0.998 |
| | 18–25 | 109.191 | 126.703 | −0.334 | 0.742 |
| | 26–40 | 129.91 | 141.935 | −0.227 | 0.823 |
| | 41–50 | 125.947 | 130.84 | −0.094 | 0.926 |
| | 51–65 | 112.133 | 94.755 | 0.388 | 0.702 |
| | Over 65 | 58.976 | 29.043 | 1.28 | 0.218 |
| Computer scams | Under 18 | 0.035 | 0.028 | 0.172 | 0.865 |
| | 18–25 | 3.27 | 4.344 | −0.216 | 0.831 |
| | 26–40 | 3.564 | 3.976 | −0.085 | 0.933 |
| | 41–50 | 3.31 | 3.759 | −0.099 | 0.922 |
| | 51–65 | 3.287 | 2.839 | 0.113 | 0.911 |
| | Over 65 | 1.853 | 0.88 | 0.521 | 0.610 |
| Other scams | Under 18 | 2.613 | 1.717 | 1.706 | 0.103 |
| | 18–25 | 143.557 | 136.569 | 0.155 | 0.878 |
| | 26–40 | 138.007 | 112.032 | 0.67 | 0.510 |
| | 41–50 | 121.104 | 98.978 | 0.586 | 0.564 |
| | 51–65 | 87.403 | 61.068 | 0.933 | 0.361 |
| | Over 65 | 34.727 | 15.856 | 1.627 | 0.123 |

Mean victimization rates per 100,000 inhabitants are presented for men and women across six age groups. Independent samples *t*-tests were performed to assess statistical significance.

In contrast, mean rates were high across most adult age groups. Among individuals aged 18 to 25, the mean rate for men was 109.19 cases per 100,000 population, compared to 126.70 for women (t = −0.334, $p$ = 0.742). In the 26–40 age group, the mean rate for men was 129.91 and for women 141.93 (t = −0.227, $p$ = 0.823), while in the 41–50 age group, men had a mean rate of 125.95 and women 130.84 (t = −0.094, $p$ = 0.926). These differences were minimal and not statistically significant. Similarly, in the 51- to 65-year-old group, men recorded 112.13 and women 94.75 (t = 0.388, $p$ = 0.702), again with no significant differences. Finally, for those aged 65 and over, the mean rate of card and check fraud was clearly higher among men (58.98) than among women (29.04), but the difference was also not significant (t = 1.280, $p$ = 0.218).

Similar patterns were observed for all other types of fraud (bank, computer, and other). None of the sex-based comparisons showed statistically significant differences across all combinations of fraud type and age group examined (all $p$-values > 0.05).

### *3.10. Projected Trends in Computer Fraud Rates by Sex and Age (2011–2035)*

The temporal patterns of computer fraud in Spain reveal marked differences by age and sex over 2011–2022, with linear projections extending to 2035 (Figure 6).

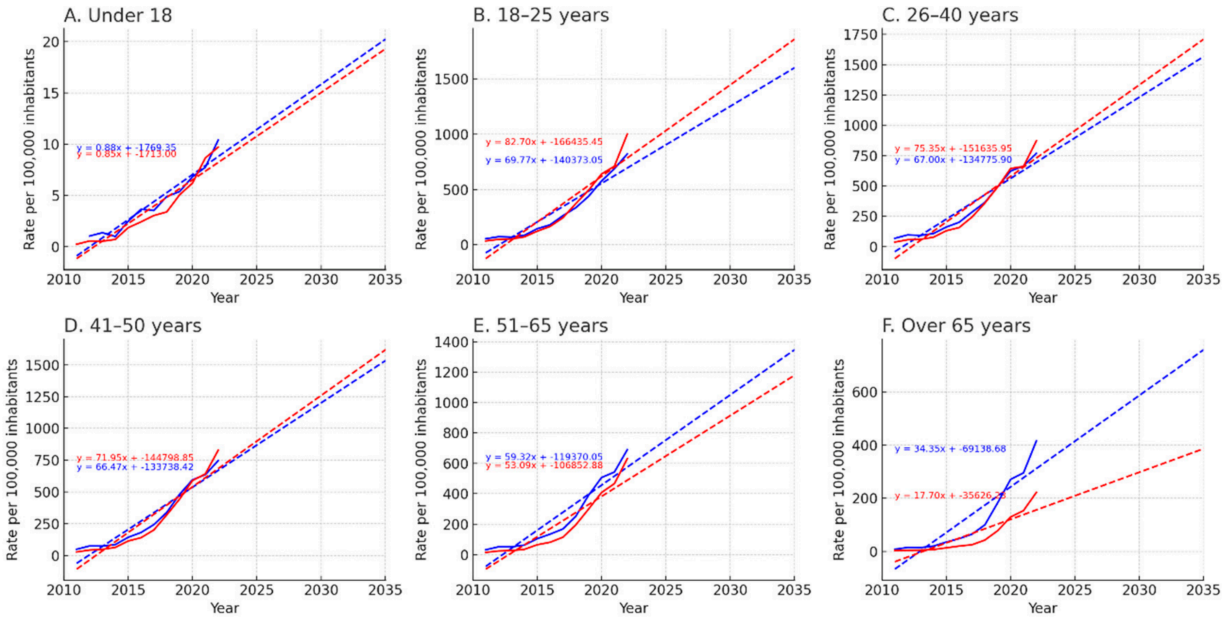



**Figure 6.** Total computer fraud rate by age group and sex in Spain (2011–2022, projected to 2035). Temporal trends and projections of computer fraud in Spain by sex and age group (2011–2035). Rates per 100,000 inhabitants are displayed for men (blue) and women (red) across six age groups: (**A**) under 18, (**B**) 18–25 years, (**C**) 26–40 years, (**D**) 41–50 years, (**E**) 51–65 years, and (**F**) over 65 years. Solid lines represent observed data (2011–2022), while dashed lines indicate linear projections up to 2035. Regression equations are shown for each subgroup.

In Figure 6A, which shows individuals under 18, both sexes show a moderate increase, but the trend is notably steeper among females ($y = 2.55x - 5076.91$) than among males ($y = 0.95x - 1895.09$). Although absolute rates remain relatively low in this age group, the sharp rise among girls suggests an especially pronounced relative increase. The gap between sexes widens significantly in the 18–25 age group (Figure 6B). Women exhibit much higher fraud rates, with a slope of 0.18 ($y = 0.18x - 362.64$) versus just 0.05 among men ($y = 0.05x - 108.29$), indicating a rapid acceleration in fraud victimization among young adult females. This trend is even more evident in Figure 6C, representing the 26–40 group, where female rates follow an upward trajectory ($y = 0.25x - 507.69$). In contrast, male rates remain flat ($y = 0.00x + 0.00$), suggesting a potential plateau in this male subgroup. The same dynamic persists in Figure 6D (41–50 years), where women continue to lead the increase in fraud rates, with a slope of 0.22 ($y = 0.22x - 435.16$) versus 0.05 for men ($y = 0.05x - 108.29$), suggesting a potential increase in female victimization in future projections. However, observed differences between sexes remain statistically non-significant. In Figure 6E (51–65 years), men show no growth ($y = 0.00x + 0.00$), while women display a significantly steeper projection ($y = 0.33x - 652.75$), consolidating a gap that is not only statistically relevant but also socially significant, given the implications in terms of digital vulnerability. Finally, Figure 6F (over 65 years) shows slower increase rates for both sexes. However, women again surpass men in slope ($y = 0.15x - 290.11$ vs. $y = 0.08x - 162.44$).

## 4. Discussion

This study examined the temporal evolution, regional disparities, and structural determinants of computer fraud in Spain, as well as its projected trends through 2035. Taken together, the findings indicate that computer fraud operates as a socio-technical and territorial system in which digital infrastructures, economic activity, user behavior, and institutional conditions interact to shape uneven patterns of exposure and growth. In this context, fraud cannot be explained by single-factor effects, but rather by the interaction between digital, socioeconomic, and territorial dimensions. Regions with higher connectivity and economic development are not only more digitally integrated but also more exposed to complex financial ecosystems, increasing opportunities for fraud. At the same time, territorial differences in reporting capacity and institutional response further modulate observed incidence rates, resulting in heterogeneous vulnerability patterns across regions. This integrative approach represents a key contribution of the present study, as it moves beyond single-factor explanations and provides a system-level understanding of computer fraud that simultaneously incorporates temporal, territorial, and structural dimensions. Accordingly, the following discussion interprets these empirical patterns and explains the underlying mechanisms within a socio-technical systems framework.

These findings reinforce the interpretation of computer fraud as an emergent property of a socio-technical system, in which digital expansion does not simply increase the number of online users but also reshapes the structure of exposure, opportunity, and vulnerability. Connectivity, income, technological access, and territorial conditions should therefore not be interpreted as isolated predictors, but as interacting components that generate cumulative risk environments. From this perspective, higher fraud rates in more developed and digitalized regions do not contradict socioeconomic progress; rather, they reflect the greater intensity of digitally mediated financial and social interactions in these territories.

Our results show that computer fraud has sustained and accelerated growth across all autonomous communities. This sustained increase may be explained by the rapid expansion of digital infrastructures and online financial services, which increases both exposure to fraud opportunities and the scale at which such offenses can be executed. Our data also reveal firm regional heterogeneity: the highest rates were concentrated in regions with higher income levels and digital penetration (Basque Country, Balearic Islands, Catalonia), while less developed regions displayed lower figures. Madrid experienced accelerated growth from 2017 to 2022, suggesting that regional rankings may shift in the future. Rather than representing isolated local anomalies, these regional disparities can be interpreted as differences in the configuration of socio-technical systems, in which connectivity, digital financial activity, economic resources, institutional capacity, and reporting practices interact to shape distinct levels of fraud exposure.

This interpretation also helps explain why territorial disparities persist despite a common national legal framework. Regional differences may reflect not only variation in fraud exposure, but also differences in reporting practices, institutional capacity, digital banking penetration, and public awareness of cybercrime. Thus, the observed regional patterns should be understood as the result of both actual victimization dynamics and the capacity of each territorial system to detect, classify, and report computer fraud.

This pattern suggests that technological development increases opportunities for victimization rather than ensuring greater security [15,23]. Other studies confirm these observations, showing that the rapid expansion of digital adoption and online financial services has created new opportunities for fraudulent activity and significantly increased consumer exposure to cybercrime [21,24]. McKinsey & Company (2022) [25] highlights that fraud has escalated as digital adoption has accelerated, enabling new and more sophisticated schemes, while Kubilay et al. (2023) [26] emphasize that the spread of digital

financial services has raised serious consumer protection concerns, particularly fraud and scams. Recent reports at the European level also stress that fraud has become the most frequently reported crime type, driven mainly by the proliferation of online platforms and services [27].

From a sociodemographic perspective, our findings show that young adults (18–25 years) were the most affected group, followed by middle-aged adults, while those over 65 years, although initially less exposed, recorded a sustained increase over the last decade. These results confirm the progressive reduction in the so-called "age protection gap" in Spain, a phenomenon documented in other contexts as well [11,28]. Our study also found no statistically significant differences between men and women, suggesting a balanced pattern of victimization by sex. However, other authors have noted that specific subtypes of fraud, such as romance fraud, disproportionately affect women [12,29], introducing relevant qualitative nuances. From a structural standpoint, our correlational analyses indicated that fraud risk is associated with broadband access, intensive internet use, and mobile device availability. These findings suggest that digital connectivity acts as a structural driver of fraud exposure, as increased access to online environments expands both legitimate and illicit interactions within the digital economy. Rather than acting independently, these factors appear to form part of an interconnected socio-technical environment in which greater digital integration may expand opportunities for fraud. Conversely, more traditional technologies, such as landline telephony, were associated with a lower incidence, suggesting a different exposure profile [25]. We also found a positive correlation with educational attainment and income levels, indicating that fraud is not limited to conventionally vulnerable groups but may be facilitated by higher levels of participation in digitally mediated economic activity. This relationship can be interpreted in terms of differential exposure to digital environments. Higher educational attainment may be associated with greater use of online financial services, digital platforms, and complex economic transactions, thereby increasing exposure to fraud opportunities. In contrast, intermediate educational levels may reflect lower engagement with these systems. Thus, education should not be interpreted as a simple protective factor, but as a variable that interacts with digital behavior and economic activity to shape vulnerability profiles. These findings should be interpreted as correlational patterns rather than causal relationships, reflecting structural associations within the socio-technical system. Thus, education should not be interpreted as a simple protective factor, but as a variable that interacts with digital behavior and economic activity to shape vulnerability profiles. These findings should be interpreted as correlational patterns rather than causal relationships, reflecting structural associations within the socio-technical system.

These results are consistent with the warnings of international bodies, which stress the need to consider demographic and structural factors when designing vulnerability profiles [26]. Finally, our results confirm that fraud incidence will continue to rise if no specific measures are implemented, as indicated by the linear projections through 2035. This projected growth suggests that, in the absence of structural interventions, the underlying drivers of the system, digital expansion, financial integration, and uneven territorial vulnerability, may continue to amplify fraud dynamics over time.

These conclusions place the Spanish experience within the broader European context, where digital fraud is the most frequently reported crime type [30]. A study further highlights that the phenomenon is accompanied by a prominent "dark figure," as a significant proportion of incidents go unreported, limiting the ability of official statistics to capture its true magnitude [31]. Our study provides empirical evidence specific to Spain, identifying territorial inequalities and sociodemographic and structural profiles of victimization. These findings reinforce the notion that computer fraud is a complex, structural, and expanding

phenomenon, whose prevention requires tailored policies by region, age, and level of digitalization [29,32]. From a systems perspective, this implies the need for adaptive, multi-level governance strategies to strengthen system resilience, reduce structural exposure, and improve coordination among technological, legal, financial, and educational responses. In practical terms, prevention strategies should be adapted to different regional profiles. Highly digitalized regions with high fraud incidence may require advanced monitoring systems, stronger cooperation between financial institutions and law enforcement agencies, and rapid-response mechanisms for emerging fraud modalities. In contrast, regions with lower digital development may benefit more from preventive interventions focused on digital literacy, safe online financial behavior, and early user protection. Intermediate regions may require hybrid strategies combining technological surveillance with educational and awareness-based measures.

Nevertheless, several limitations should be noted. First, our data are derived from official police records, which are subject to underreporting and may underestimate the true magnitude of computer fraud due to the well-known dark figure of crime, as many incidents remain unreported or undetected. In addition, future research may benefit from triangulating official police data with alternative sources, such as victimization surveys, financial sector reports, or cybersecurity datasets, to improve the accuracy and completeness of fraud estimates. Second, differences in the timing and completeness of police reporting systems between regions may introduce comparative biases. Catalonia and the Basque Country incorporated their records into the national system later, which may have affected the series' temporal comparability. This delayed inclusion may introduce measurement bias and artificially inflate recorded fraud rates, affecting temporal comparability and potentially overstating growth trends in certain regions. In addition, projections to 2035 are based on the continuation of current trends and do not account for potential policies, technological, or behavioral changes, which introduce uncertainty and may affect the accuracy of future estimates.

Finally, the associations identified with socioeconomic and technological factors are correlational and do not imply causality. In addition, the present study does not explicitly model feedback mechanisms, non-linear dynamics, or causal interdependencies among variables. Future research should address these limitations by applying advanced analytical approaches, such as multivariate regression models, longitudinal designs, and dynamic or network-based methods, to better capture causal relationships and system interactions. Additionally, K-means clustering may be sensitive to initial conditions and does not capture temporal dynamics, which may affect the stability and interpretation of the identified regional groupings. Therefore, these results should be considered exploratory, and future research should incorporate alternative clustering methods and stability analyses to validate these patterns. Furthermore, the use of bivariate correlations without control variables may introduce bias due to unobserved confounding factors, and therefore, the observed associations should be interpreted as exploratory rather than causal.

## 5. Conclusions

This study shows that computer fraud in Spain is not merely a growing form of cybercrime, but a socio-technical and territorial phenomenon shaped by the interaction of digital, economic, and structural factors. By integrating temporal trends, regional disparities, clustering patterns, demographic profiles, and structural associations, the study provides a system-level framework for understanding how fraud vulnerability emerges across territories. The findings support the need for differentiated and adaptive prevention strategies. Highly digitalized regions may require advanced detection systems, real-time monitoring, and stronger financial cybersecurity infrastructures, whereas less digitally

developed regions may benefit from digital literacy programs, awareness campaigns, and basic user-protection measures. Intermediate regions may require combined approaches adapted to transitional vulnerability profiles.

Overall, addressing computer fraud requires coordinated action across technological, regulatory, financial, and educational domains. Future policies should move beyond uniform national responses and incorporate regional vulnerability profiles to improve prevention, detection, and system resilience.

**Author Contributions:** Conceptualization, C.J.M. and I.L.; methodology. C.J.M. and I.L.; software, C.J.M. and I.L.; validation, C.J.M., I.L. and A.L.; formal analysis, C.J.M., I.L. and A.L.; investigation, C.J.M., I.L. and A.L.; resources, C.J.M., I.L. and A.L.; data curation, C.J.M.; writing—original draft preparation, C.J.M., I.L. and A.L.; writing—review and editing, C.J.M., A.L. and I.L.; visualization, C.J.M., I.L. and A.L.; supervision, I.L. and A.L.; project administration, I.L.; funding acquisition, I.L. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

**Conflicts of Interest:** The authors declare that the research was conducted without any commercial or financial relationships that could be construed as a potential conflict of interest.

## References

1. Bitaab, M.; Cho, H.; Oest, A.; Zhang, P.; Sun, Z.; Pourmohamad, R.; Kim, D.; Bao, T.; Wang, R.; Shoshitaishvili, Y.; et al. Scam Pandemic: How Attackers Exploit Public Fear through Phishing. In *2020 APWG Symposium on Electronic Crime Research (eCrime)*; IEEE: Piscataway, NJ, USA, 2021. [CrossRef]
2. Van De Weijer, S.G.A.; Leukfeldt, R.; Bernasco, W. VU Research Portal Determinants of Reporting Cybercrime. *Eur. J. Criminol.* **2018**, *16*, 486. [CrossRef]
3. Aebi, M.F.; Miró-Llinares, F.; Caneppele, S. *Understanding Crime Trends in a Hybrid Society*; SpringerBriefs in Criminology; Springer: Cham, Switzerland, 2025.
4. Muñoz-Quirós Caballero, J.M.; Alberola, S.G. Manual de Medicina y Toxicología Forense-Dialnet. Available online: https://dialnet.unirioja.es/servlet/libro?codigo=662597 (accessed on 30 June 2020).
5. Balani, H. Corporate Digital Identity: Revolutionizing Financial Crime Prevention in Banking. *SSRN Electron. J.* **2024**. [CrossRef]
6. Koning, L.; Junger, M.; Veldkamp, B. Reporting Fraud Victimization to the Police: Factors That Affect Whether Victims Report. *Psychol. Crime Law* **2025**, 1–29. [CrossRef]
7. Directive-2013/40-EN-EUR-Lex. Available online: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (accessed on 25 August 2025).
8. BOE-A-2015-3439. Ley Orgánica 1/2015, de 30 de Marzo, Por La Que Se Modifica La Ley Orgánica 10/1995, de 23 de Noviembre, Del Código Penal. Available online: https://www.boe.es/eli/es/lo/2015/03/30/1 (accessed on 22 August 2025).
9. Internet Organised Crime Threat Assessment (IOCTA) 2023. Europol. Available online: https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023 (accessed on 12 May 2025).
10. Home. Europol. Available online: https://www.europol.europa.eu/ (accessed on 24 August 2025).
11. Button, M.; Nicholls, C.M.N.; Kerr, J.; Owen, R. Online Frauds: Learning from Victims Why They Fall for These Scams. *Aust. N. Zeal. J. Criminol.* **2014**, *47*, 391–408. [CrossRef]
12. Whitty, M.T. Do You Love Me? Psychological Characteristics of Romance Scam Victims. *Cyberpsychol. Behav. Soc. Netw.* **2018**, *21*, 105. [CrossRef] [PubMed]
13. Abubakari, Y. The Espouse of Women in the Online Romance Fraud World: Role of Sociocultural Experiences and Digital Technologies. *Deviant Behav.* **2024**, *45*, 708–735. [CrossRef]
14. Portal Estadístico de Criminalidad. Available online: https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/datos.html?type=pcaxis&path=/Datos5/&file=pcaxis (accessed on 14 March 2025).
15. Spanish Statistical Office. Available online: https://www.ine.es/en/ (accessed on 17 September 2022).
16. Población de 16 y Más Años Por Nivel de Formación Alcanzado, Sexo y Comunidad Autónoma. Porcentajes Respecto Del Total de Cada Comunidad(6369). Available online: https://www.ine.es/jaxiT3/Datos.htm?t=6369#_tabs-grafico (accessed on 29 April 2025).
17. Nota de Prensa: Atlas de Distribución de Renta de Los Hogares. Año 2022. Available online: https://www.ine.es/dyngs/Prensa/ADRH2022.htm (accessed on 9 May 2025).

18. La Estrategia de La UE Sobre Los Derechos Del Niño y La Garantía Infantil Europea-Comisión Europea. Available online: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/rights-child/eu-strategy-rights-child-and-european-child-guarantee_es (accessed on 29 April 2025).
19. Evolución de Datos de Viviendas (2006–2024) Por Tamaño Del Hogar, Hábitat, Tipo de Equipamiento y Periodo. Available online: https://www.ine.es/jaxi/Datos.htm?tpx=70391#_tabs-tabla (accessed on 6 May 2025).
20. BOE-A-1995-25444 Ley Orgánica 10/1995, de 23 de Noviembre, Del Código Penal. Available online: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 (accessed on 22 August 2025).
21. Bock, H.-H. Clustering Methods: A History of k-Means Algorithms. In *Selected Contributions in Data Analysis and Classification*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 161–172. [CrossRef]
22. STS 457/2020, 24 de Julio de 2020-VLex España. Available online: https://vlex.es/vid/846978599 (accessed on 22 August 2025).
23. *ISO 3166*; Country Codes. ISO: Geneva, Switzerland, 2020. Available online: https://www.iso.org/iso-3166-country-codes.html#2012_iso3166-2 (accessed on 14 March 2025).
24. Syakur, M.A.; Khotimah, B.K.; Rochman, E.M.S.; Satoto, B.D. Integration K-Means Clustering Method and Elbow Method For Identification of the Best Customer Profile Cluster. *IOP Conf. Ser. Mater. Sci. Eng.* **2018**, *336*, 012017. [CrossRef]
25. A New Approach to Fighting Fraud While Enhancing Customer Experience. McKinsey. Available online: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-new-approach-to-fighting-fraud-while-enhancing-customer-experience (accessed on 25 August 2025).
26. Kubilay, E.; Raiber, E.; Spantig, L.; Cahlíková, J.; Kaaria, L. *Financial Fraud in Developing Countries: Common Scam Detection Tips Do Not Help Distinguish Scam from Non-Scam Messages*; Reinhard Selten Institute: Bonn, Germany, 2023.
27. Afzal, M.; Meraj, M.; Kaur, M.; Shamim Ansari, M. How Does Cybersecurity Awareness Help in Achieving Digital Financial Inclusion in Rural India under Escalating Cyber Fraud Scenario? *J. Cyber Secur. Technol.* **2025**, *9*, 88–126. [CrossRef]
28. Kraemer-Mbula, E.; Tang, P.; Rush, H. The Cybercrime Ecosystem: Online Innovation in the Shadows? *Technol. Forecast. Soc. Change* **2013**, *80*, 541–555. [CrossRef]
29. Rothman, K.J. Epidemiological Evidence on Health Risks of Cellular Telephones. *Lancet* **2000**, *356*, 1837–1840. [CrossRef]
30. Crime in England and Wales: Year Ending June 2024. Office for National Statistics. Available online: https://www.ons.gov.uk/releases/crimeinenglandandwalesyearendingjune2024 (accessed on 25 August 2025).
31. Holtfreter, K.; Reisig, M.D.; Pratt, T.C. Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology* **2008**, *46*, 189–220. [CrossRef]
32. ENISA Threat Landscape 2024. ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (accessed on 24 August 2025).


**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.