Facing online scams: The bait of low-effort rewards among adolescents and parents

Abstract

Purpose – This study aims to investigate adolescents' interactions with deceptive content on social media, focusing on scams that promise effortless rewards.

Design/methodology – The methodology included interviews with 20 pairs of adolescents (aged 11 to 17) and their parents, analyzing their responses to scam content and examining patterns of critical awareness and parental guidance.

Findings – Findings suggest that critical awareness and the ability to identify scams improve with age. Primary school individuals rely heavily on parental guidance, whereas adolescents in high schools' exhibit increased critical thinking, largely because of systematic education about online risks. Parents of younger participants are more concerned and emphasize supervision, while those of older participants display greater confidence in their children's capabilities.

Practical implications – This study recommends comprehensive educational programs to develop critical awareness among adolescents. Suggested strategies include implementing school-based curricula on digital literacy, organizing parental workshops to encourage active supervision, and fostering collaboration with social media platforms to promote awareness campaigns.

Originality/value – This research highlights the changing role of adolescents as both targets and potential spreaders of fraudulent content on social media. This study expands the understanding of how these demographics navigate online risks and contributes to the broader discourse on social media misinformation.

Keywords: scams, social media, online risks, critical thinking, parental perception, fraudulent content

1. Introduction

Online scams are a pervasive and evolving threat to the digital environment. The 2022 Global State of Scams report (Group-IB, 2022) estimates losses exceeding $10 billion in the United States, with Spain ranking among the ten most affected countries. Beyond financial damage, scams frequently involve emotional manipulation, including romantic deception, impersonation, and identity theft, leading to lasting psychological consequences (Cross and Layt, 2022). While scams target all demographics, adolescents remain particularly vulnerable because of their developmental stage and limited experience in detecting deception. Understanding scam mechanisms and their impact is essential for evaluating how adolescents and their parents perceive and respond to digital risk.

Fraud and scams are often used interchangeably, yet they have distinct meanings. Fraud, as defined by Button and Cross (2017), encompasses a broad range of reality-manipulating activities designed to secure personal advantages or harm others. Scams, a subset of fraud, specifically involve deceptive schemes that extract money or personal information and often constitute civil, regulatory, or criminal offenses.

Adolescence represents a transitional phase from childhood to adulthood, marked by biological, psychological, and sociocultural changes (Tanner, 1973). This stage, typically spanning ages 11-18 (Stanley-Hall, 1904), can extend into early adulthood, shaped by neurodevelopmental milestones and broader societal influences (Feixa, 2011). Cognitive development during this period includes significant advancements in executive functions such as decision-making, risk assessment, and impulse control (Steinberg, 2005). However, these abilities develop unevenly, leaving early adolescents (11-14 years) reliant on concrete operational thinking, which limits their ability to anticipate long-term consequences or to recognize subtle online manipulations. Older adolescents (15-18 years), while more capable of abstract reasoning, remain susceptible

to impulsivity and emotional reactivity owing to asynchronous maturation of the limbic system and prefrontal cortex (Demurie *et al.,* 2025).

Neurochemical changes in the dopaminergic system heighten adolescents' sensitivity to social rewards and peer validation, increasing their vulnerability to persuasive tactics such as social proof or appeals to authority (Boone *et al.,* 2025). This heightened sensitivity coupled with a tendency to seek novel experiences reduces their ability to critically evaluate risks in online interactions (Vente *et al.,* 2020).

Environmental pressures such as low parental supervision, economic stress, or familial conflict may further increase the likelihood of manipulative or deceptive behavior—sometimes as a social coping mechanism (Ohu & Jones, 2025; Ceroni & Yalch, 2024). Researchers have identified validation syndrome as a key driver of adolescents' engagement in both deceptive practices and their vulnerability to online manipulation. When these cognitive limitations are compounded by socioeconomic disadvantages or weaker learning abilities, as shown in Jerrim (2023), the likelihood of falling victim to phishing and other forms of online fraud increases significantly. This intersection of neurodevelopmental immaturity and structural inequality creates specific mechanisms of vulnerability that digital scams can easily exploit.

Given these developmental characteristics, adolescents often lack the cognitive and emotional resources needed to effectively identify and respond to online scams (Paat and Markham, 2021). Research has examined adolescent online risks, including digital sexuality (Landry *et al.,* 2017), mental health concerns (O'Reilly, 2020), internet addiction (Akdeniz-Kudubes and Sezer-Efe, 2023), and body image disorders (Saul *et al.,* 2022). However, scams and fraud remain relatively understudied, even though it is a latent risk in their online experience (Shin and Lwin, 2017). According to the latest Cybercrime Report (Ministry of the Interior*, 2023*), the most prevalent category of cybercrime targeting minors is threats and coercion, which tops the list of offenses

committed against individuals under the age of 18. The second most frequently reported cybercrime affecting this age group is online fraud, highlighting the growing vulnerability of minors to online scams and deceptive digital practices. This gap highlights the importance of understanding adolescent vulnerabilities to online deception.

Scammers exploit adolescent vulnerabilities by leveraging trust in their digital networks. For example, adolescents frequently share passwords with their peers, increasing the risk of identity theft (El-Asam and Katz, 2018). Whitty (2013) found that adolescents are highly susceptible to promising rewards in exchange for personal information, which can then be used for fraudulent purposes. This vulnerability is particularly pronounced on entertainment and gaming platforms, where fraudulent in-game purchases and subscription scams thrive (Feijoo *et al.,* 2021).

Despite these risks, scams targeting adolescents have received less academic attention than other online threats (Garitaonandia *et al.,* 2020). Paat and Markham (2020) argued that scams remain a significant yet under-recognized issue, necessitating greater involvement from families, educational institutions, and digital platforms.

This study examines how adolescents and their parents perceive the risks of online scams, particularly in the context of fraudulent social media posts that promote low-effort rewards. By analyzing adolescents' ability to identify deceptive content and assess parental awareness of their children's critical digital literacy, this research explores the dynamics shaping adolescent susceptibility to scams.

1.1. Adolescence vulnerability and susceptibility to online scams

Digital platforms offer vast resources and pose significant challenges (Nemilentseva et al., 2024). Users face misinformation, deepfakes, and manipulative content, whereas generative AI and algorithms blur credibility (Christakis and Hale, 2025). Adolescents

who develop critical thinking skills and high digital exposure, are especially vulnerable to sophisticated online scams.

Scam perpetrators exploit individuals' social and technical vulnerabilities (Jagatic *et al.,* 2017). Social media provides cybercriminals with ample opportunities to gather data about individuals' interests, occupations, close networks, and geographic locations, making scams increasingly personalized and effective (Hong, 2012). According to Parti (2023), adolescents are the most active users on these platforms, rendering them prime targets for innovative scams.

Besides vulnerability, susceptibility to online scams also plays a significant role in the victimization of adolescents (Guerra and Taylor, 2021). In psychology, it is posited that susceptibility to scams is influenced by three complementary but independent factors: (a) the persuasive techniques used by the sender, (b) the user's information processing, and (c) individual characteristics (Jones *et al.,* 2019).

Adolescents are highly vulnerable to scammers' persuasive techniques (Xie & Duan, 2025), which exploit psychological principles to manipulate behavior. "Dark patterns" play a key role, using deceptive design to influence decisions individuals might not make if fully informed or autonomous (Kollmer and Eckhardt, 2023). These techniques have been extensively analyzed over the years (Workman, 2008; Guerra and Taylor, 2021; Xie and Duan, 2025) and include (1) impersonating trusted figures, (2) creating friendly personas, (3) promoting conformity, (4) encouraging small commitments, (5) fostering reciprocity through gifts, (6) inducing urgency with scarcity, (7) promising financial or psychological rewards, and (8) emphasizing potential losses to pressure victims into action. These strategies exploit psychological tendencies, making individuals more susceptible to online deception and manipulation.

Some studies indicate that adolescents are significantly more likely to fall victim to scams than are adults. Common scams targeting this demographic include personal data

verification, identity theft, deceptive reward schemes, advance fee fraud, and romantic scams (Parti, 2023). Additionally, Guerra and Taylor (2021) highlighted phishing schemes disguised as school-related communications, fake scholarship offers, and bogus contests targeting young users. Xie and Duan (2025) also emphasize scams exploiting adolescents' interest in gaming and entertainment platforms, such as fake in-game purchases, fraudulent subscription services, and counterfeit giveaways (Figure 1). [Figure 1].

An interesting contribution on cybersecurity is the Foundational Digital Literacy and Cybersecurity Awareness Skills model (Piliouras *et al.,* 2025). The authors place emphasis on a structured, skills-based approach to digital literacy that directly addresses online scams and deception. Their framework highlights the importance of Social Engineering Awareness as a core competency, equipping learners to detect phishing, deepfakes, and other manipulation tactics commonly used in cyber fraud. Equally significant is the inclusion of Privacy and Data Protection as a defense against identity-based scams and introduce AI and Cybersecurity Ethics to encourage reflection on the manipulative potential of emerging technologies.

Given adolescents' vulnerabilities, parental perception is crucial in fostering the skills and awareness needed to navigate social media risks safely.

1.2. Parental perception and adolescence safety in the face of social media risks

As social media platforms have evolved, adolescents increasingly engage in online interactions without fully understanding the security and privacy risks. This lack of awareness contributes to cyberbullying (Hong *et al.,* 2025), identity theft (Lareki *et al.,* 2017), and susceptibility to online scams (Parti, 2023). In response, parental mediation has emerged as a crucial strategy for monitoring and guiding children's digital activities

(Sela *et al.,* 2025). Research has indicated that active parental involvement can significantly reduce online risk (Salazar *et al.,* 2025).

Parental mediation encompasses various strategies, including screen time restrictions, the direct supervision of online content, and open discussions about responsible technology use (Shin and Kang, 2016). Studies suggest that adolescents who receive guidance from engaged parents are less likely to recklessly share personal information (Soyoof *et al.,* 2024). Additionally, fostering adolescents' awareness of online risks helps them develop safer digital habits (Cohen-Zilka, 2017). However, despite providing their children with digital devices, many parents lack technical knowledge to protect them from specific dangers, such as online grooming (Dorasamy *et al.,* 2021). Emotional intelligence also plays a role in mediating effectiveness, as parents with higher emotional awareness are better equipped to help their children recognize and manage risks (Mueller *et al.,* 2020).

Effective mediation depends on open communication between parents and adolescents (Wisniewski *et al.,* 2016). Some families struggle to provide adequate support regarding specific risks, including online contact with strangers and financial scams (Quayyum *et al.,* 2021). Although many parents possess a general understanding of cyber threats, they often lack in-depth knowledge (Abayomi-Aborisade, 2022) and may not fully acknowledge their role in mitigating risks (Abdul-Morok *et al.,* 2023).

The reactions of adolescents to parental mediation are diverse. While younger children may be more accepting of oversight, older adolescents often perceive it as restrictive and invasive (Wisniewski *et al.,* 2025). These perceptions influence the effectiveness of parental strategies, as excessive control may hinder adolescents' development of autonomy and critical thinking skills (Dedkova and Mýlek, 2023).

These insights highlight the relevance of exploring how adolescents engage in persuasive and fraudulent online content through both individual reasoning and their

interactions with parents. Digital risks are intertwined with developmental, emotional, and educational factors, making it crucial to consider adolescent agency alongside parental mediation. To explore these dynamics, we focused on how families perceive and respond to scams as promising effortless rewards on social media.

2. Objective and research questions

The objective of this research is to understand the perceptions and evaluations that adolescents and their parents have regarding exposure to social media scams. Additionally, examines the reactions and questioning by parents and children to fraudulent posts that promote low-effort rewards, as well as the extent of adults' knowledge about their adolescents' critical capacity concerning such content. The research questions guiding the study are:

RQ1: What are the perceptions of adolescents and their parents about the propagation of scams on social media?

RQ2: How do parents and children demonstrate critical awareness of such fraudulent content?

RQ3: What are parents' perceptions of their children's critical capacity in relation to these scams on social media?

3. Methodology and sample

To address the research questions, dyadic interviews were conducted with 20 adolescents (aged 11–17 years) and one of their parents, recognizing parents as primary influencers in adolescents' critical competency development. This study is part of a broader project conducted in two phases.

The first phase involved 12 focus groups with 62 adolescent social media users assessing their ability to identify and interpret different content types (informative,

educational, and persuasive). The second phase, forming the basis of this study, included semi-structured interviews with 20 participants from focus groups. To gain a comprehensive perspective, their parents were interviewed as they play a key role in shaping critical thinking skills.

We performed 20 paired interviews, selecting participants based on socioeconomic status (high, medium, low) and age group, ensuring representation across educational stages (6th grade of Primary, 1st and 2nd cycles of ESO, and Baccalaureate). These categories align with international educational systems, which presents the stage equivalencies between Spain, the United Kingdom, and the United States (Table 1).

[Table 1]

The dual segmentation approach was chosen to account for the influence of both age and socioeconomic background on adolescents' critical competence levels. Participants were recruited from schools across Spain, including Galicia and Asturias (North), Madrid (Center), Andalusia (South), and Catalonia and the Valencian Community (East). Socioeconomic classification considered school type (private, semi-private, or public), the surrounding area's income levels, and parents' employment status. Fieldwork took place during the first quarter of 2022.

The final sample comprised 11 girls and 9 boys, with an average age of 14. Participants were distributed across educational stages: four in 6th grade of Primary, six in the 1st cycle of ESO, eight in the 2nd cycle of ESO, and two in Baccalaureate.

Among the 20 interviewed parents, the average age was 45 years, with mothers representing the majority (*n*=16). Families varied in socioeconomic status: five were high-income (over €30,000), ten middle-income (€11,450–€30,350), and five low-income (below €11,450), based on Spanish National Institute of Statistics data (Andrino *et al.,* 2021). This segmentation ensured a diverse representation of adolescent experiences and parental perspectives on digital literacy and online scams.

3.1. Semi-structured interviews

We conducted semi-structured online interviews via Zoom, first with the adolescents and then with their parents. Each interview lasted for 30–35 minutes. To ensure independent responses, the participants were interviewed separately, with instructions to remain in different rooms to prevent mutual influence. Parents provided an informed consent and adolescents provided verbal consent. The study was approved by the university's Ethics Committee (details withheld for peer review).

A structured script explored participants' perceptions of social media use, risks, and opportunities with a focus on online scams. To assess critical awareness, two real Instagram posts were shown as examples. This situational approach has moved beyond dispositional analysis (Hudders *et al.,* 2017).

The first example featured a fraudulent post from an unofficial account of a well-known clothing brand, offering free products to users with at least 200 followers as "brand ambassadors". The second, resembling a pyramid scheme, promised financial rewards for travel, requiring a €100 monthly investment and recruitment of new members for cruise discounts. These examples gauged participants' ability to recognize deceptive tactics (Table 2).

[Table 2]

3.2. Data analysis

We analyzed the interviews using a grounded theory approach (Corbin and Strauss, 2008), which allowed us to inductively identify patterns and generate categories rooted in participants' narratives. To support the coding process, we employed the AI-based coding function of qualitative Atlas.ti 24 software. This tool provided an initial semantic grouping of the data segments based on lexical and contextual similarities. We manually

reviewed, refined, and redefined the AI-generated codes to ensure conceptual coherence and relevance to the study aims.

As the analysis progressed, we iteratively contrasted new data segments with existing codes to refine the categories and eliminate overlaps. Rather than generating themes independently from the data, we used the study's three research questions as a conceptual framework to organize and interpret the emerging categories. This structure allowed us to maintain a clear analytical focus while remaining grounded in participants' lived experiences. In addition, theoretical saturation guided endpoint analysis. Once the final interviews no longer produced novel insights, we considered the category system that we developed. Thus, the integration of AI-supported coding contributed to data handling, but analytic decisions were entirely human-led, preserving inductive logic and methodological rigor central to grounded theory.

We conducted the full analysis process as a single researcher, following grounded theory's emphasis on maintaining interpretive consistency and analytic depth through iterative engagement with data (Charmaz, 2014). This approach facilitated theoretical sensitivity and cohesion, as it enabled sustained and reflective dialogue between the researcher and data.

4. Results

4.1. RQ1: Parents' and adolescents' perceptions of social media scams

Adolescents and their parents' perceptions of scams, including those soliciting brand ambassadors in exchange for free products and those offering travel at minimal costs with a monthly subscription and recruitment of new members, reflected diverse views influenced by age. These perspectives helped us understand how various age groups identify and respond to these digital deceptions, particularly those promising easy rewards for minimal effort.

4.1.1. Among youthful curiosity, doubt, and skepticism

Among primary school children, we noted a contrast between curiosity and distrust when they were presented with two scams. One student particularly identified irregularities in the message:

> *Maybe... this is a fake profile [...] because it does not look like the other one and is misspelled. [...] Because there is an 'n' there... I think it is wrong. So it may be a fake profile.* (Boy_6th_Grade_low_SES)

The comment reflects an emerging ability to detect inconsistencies in content, though his understanding of the nature of scams still appears to require further development at this age. This finding is consistent with previous research that suggests children are still developing critical skills and heavily rely on parental guidance to differentiate between reliable and unreliable information.

In secondary school, adolescents demonstrated more pronounced skepticism towards such content. One girl remarked, "*You get strange messages but you do not open them*" (Girl_1st_Cycle_ESO_medium_SES), indicating a cautious awareness of messages that seem "incoherent" or "suspicious". High school students exhibited a more advanced capacity to recognize and evaluate online scams, leading to their immediate dismissal. Some expressed bafflement towards individuals who readily accept such dubious messages. A girl elaborated:

> *I have unopened messages from people who tell me: 'Enter the link to I do not know what'. Please do not click on this link. [...] I mean just enter the profile and*

> *see that it has zero followers that is zero followers zero followers and no publications! Do not click on the link*. (Girl_Baccalaureate_medium_SES)

The degree of skepticism observed here aligns with findings by El-Asam and Katz (2018), who noted that adolescents develop a greater critical capacity as they gain more experience with digital content.

4.1.2. Warning and preventive parental education response to online scams

Parents' perceptions of social media scams reflect their concern for their children's safety and their keen awareness of potential risks. A mother of a primary school child expressed doubts about her son's ability to recognize scams, noting that such messages "*would probably attract his attention*" (Mother_6th_Grade_low_SES) and that he might not identify a scam without her guidance. Consequently, she always advises him not to click on or engage with any advertisements or messages received through social media. This comment underscores the perceived vulnerability of children and the critical need for parental supervision, in line with studies by Shin and Kang (2016) and Soyoof *et al.* (2024).

In secondary school, parents exhibit a mix of confidence in their children's ability to avoid these messages and some concern about their maturity. A mother of a secondary school student explained:

> *I trust her and I have told her not to contact or let anyone she does not know follow her. So let us see I am always worried about her but well. I do not think this is an imminent danger. [...] I think that those who contact her are trustworthy people*. (Mother_1st_Cycle_ESO_medium_SES)

In high school, parents appear more confident in their children's critical capacity. One father stated that his daughter has been taught to be skeptical and critical of seemingly simple offers: "*We've told her many times that things presented as easy are not really simple*" (Father_Baccalaureate_medium SES). However, he acknowledged some uncertainty about the effectiveness of this advice: "*I'm not saying it's 100 percent certain. She might still fall into a trap, but I think it's unlikely*" (Father_Baccalaureate_medium_SES). This confidence is rooted in proactive educational efforts, suggesting that family intervention and awareness of "easy rewards" are crucial in shaping children's attitudes and aptitudes towards online scams.

These observations align with the findings of Muir and Joinson (2020) and Wisniewski *et al.* (2016), who argue that open and consistent family communication can significantly enhance the identification and management of online threats. Moreover, the development of intrafamily emotional intelligence in risk situations is fundamental (Mueller *et al.,* 2020).

4.2. RQ2: Critical thinking of adolescents and parents against online scams on social media

Building on earlier perceptions, we discovered that critical awareness of fraudulent content on social media develops gradually and varies significantly between age groups, often influenced by experience with online content and home education.

For primary school children, we noted that this awareness is still at an initial stage and heavily relies on parental guidance. For example, a boy explained that the content from one of the brands "*could involve a worker looking for major influencers... Imagine: TheGrefg, Ibau, Rubius, etc. They could promote the brand and thus boost sales*" (Boy_6th_Grade_high_SES). He also mentioned that the offer seemed very tempting: "*Free clothes... I think if they make more sales thanks to you, they will continue to trust*

you. They'll call you for future opportunities" (Boy_6th_Grade_high_SES). These comments illustrate the significant influence of persuasive messages from influencers, celebrities, and trusted figures on young people.

Conversely, the same boy expressed reliance on his parents for handling potential threats: "*If I inadvertently got involved and made a mistake... I would tell my parents. My father would probably know how to handle it*" (Boy_6th_Grade_high_SES). Other participants shared experiences that demonstrated their awareness of the dangers posed by potential scams:

> *Last year someone sent me a catalog to buy some machines or I did not know what they were, and I was with friends. I showed it to them and they said: 'Block it, block it, block it now'. And I blocked it.* (1st_Cycle_ESO_medium_SES)
>
> *Many times I have been on the point of falling into this trap because you often receive messages even by SMS with giveaway offers that you won a product and you have to be sure that if you have not participated in any giveaway, you cannot win any product*. (Boy_2nd_Cycle_ESO_medium_SES)

The preadolescent demographic exhibits a more developed understanding of scam risks, consistent with research showing that adolescents are more cognizant of digital frauds and tend to verify information with family and peers before taking action (Jones *et al*., 2019).

Again, high school students exhibited a great level of critical awareness and maturity regarding these deceptions. Some pointed out that other age groups are more susceptible to these social engineering tactics:

> *Lifetime scammers, the mythical ones that call your grandmother or the elderly. They offer you I do not know what... especially to older people who have no idea. They go to younger people, I think 12 and 11 years old, who do not know much either.* (Girl_Baccalaureate_medium_SES)

In some instances, they even sought the advice of other adults to verify and compare information. For instance, one girl who received a notification about an Inditex gift card via YouTube discussed it with her mother, who advised, "*'I don't know, ask your uncle', since my uncle works at Inditex, and he informed us, 'No, that's not related to Zara or anything else'*" (Girl_Baccalaureate_medium_SES). This underscores the role of a supportive family environment in fostering and enhancing critical awareness (Wisniewski *et al*., 2016; Muir and Joinson, 2020).

Other examples demonstrated this critical approach towards scams offering easy rewards. However, they noted that, unfortunately, despite often recognizing these scams, they are not entirely immune to their effects. This has led them to exercise greater caution when engaging with suspicious messages or profiles:

> *From the very first moment I did not believe it, to be honest, because... first of all a company is not going to give you money just because they feel like it.* (Girl_Baccalaureate_medium_SES)

This level of skepticism demonstrates an internalization of the lessons on online safety and mistrust previously emphasized by their parents. These lessons appear to have shaped their ability to critically evaluate potentially deceptive scenarios online, such as scams offering effortless rewards. The reflections also suggest that skepticism is not

only a result of direct educational messages, but also a product of repeated exposure to narratives about online risks.

For example, they referenced the unrealistic nature of promises made by scammers and the manipulative strategies used to build trust, such as displaying wealth or creating a false sense of opportunity. These insights reveal that participants are actively engaging with the cognitive dissonance created by scams: while they recognize the warning signs, they also acknowledge their own vulnerabilities, such as emotional responses to persuasive messages or visual cues (Whitty, 2013; Mueller *et al.,* 2020; Feijoo *et al.,* 2021).

In the case of primary school children, parents emphasized their insistence on teaching caution regarding potentially suspicious messages received through instant messaging services like WhatsApp, social media, or other online platforms. Specifically, they advised children that the best preventive measure against the consequences of these messages was to consult an adult family member. One mother stated, "*that is what I am afraid of*" (Mother_6th_Grade_medium_SES).

At the upper levels of secondary school, parents noted that susceptibility to scams offering easy rewards could affect individuals of any age. One mother explained: "*I cannot always distinguish a scam from a legitimate offer [...] I might understand better after talking to the person who is promoting the offer, once they actually explain what they are doing*" (Mother_1st_Cycle_ESO_medium_SES).

Furthermore, they expressed concern that young people are particularly vulnerable to these tactics: "*If many adults find it difficult, just imagine a 14 or 15-year-old*" (Mother_1st_Cycle_ESO_high_SES); "*There are adults who are completely convinced by these scams. I hope she does not fall for them*" (Father_1st_Cycle_ESO_medium_SES). Parents of high school students concurred with the earlier statements, expressing their skepticism regarding the reliability of

information received through various media and technologies: "*I believe that everything that comes out of the phone, television... some things are true and some are false. That is why I am very careful*", one mother explained (Mother_Baccalaureate_medium_SES). This skepticism was particularly directed at messages promising easy rewards—such as getting money, obtaining free products, traveling for free, obtaining exclusive cards, or becoming brand ambassadors—with one mother citing the adage, "*think the worst and you will not be far wrong*" (Mother_2nd_Cycle_ESO_medium_SES). In some instances, it was the adolescents who alerted their parents to potential scams. A mother, who is also a teacher, shared:

> *I got a message on my mobile [...] that I had won an iPhone and of course I saw it and I said unusual. Older people always think well; nobody offers anything for free here. But it was my own students who told me: 'Teacher, that is a scam!' and I tell them 'And why do you know it is a scam?' And they say: 'Because if you join, you have to provide your personal information*'.
> (Mother_1st_Cycle_ESO_low_SES)

Consequently, our findings indicate that parents are both fearful and aware of the risks and vulnerabilities that adolescents face regarding online scams, vigilantly monitoring the digital content their children access. This vigilance persists into high school, where parents noted that sometimes even the adolescents alert them about potentially fraudulent messages. Thus, as adolescents gain autonomy and develop maturity in navigating online environments, they increasingly act as the primary detectors and informants of fraud.

4.3. RQ3: Parents' perceptions of their children's critical thinking skills

The exploration of parents' perceptions of their children's critical capacities revealed a significant discrepancy between parental assessments and adolescents' self-evaluations, particularly at younger ages. This gap may stem from a natural parental inclination to protect their offspring by underestimating their maturity and ability to navigate digital risks (Dorasamy *et al*., 2021).

Specifically, parents of primary and secondary school children expressed heightened concern about adolescents' susceptibility to recognized individuals or influencers:

> "*Especially if it comes from someone he admires a lot, of course*", noted one mother (Mother_6th_Grade_medium_SES); "*If someone on your Brawl Stars forum or any video game forum says 'hey, pay me this amount of money... I promise I will give you something for free,' they're just trying to bait you*", observed a father (Father_1st_Cycle ESO_medium_SES).

Consequently, they were cautious about allowing their children access to their own or other family members' Facebook or Instagram profiles, viewing such access as potentially delaying or mitigating the influence of these deceptive strategies. Another father worried, "*It's like a bait to get kids to respond; they could be a pedophile*" (Father_2nd_Cycle_ESO_low_SES), while another parent feared it could be a tactic for "*recruiting people into some kind of cult*" (Mother_2nd_Cycle_ESO_medium_SES).

As parents voiced concerns over their children's discernment, significant discrepancies emerged, particularly between preadolescents and adolescents. Some parents displayed moderate confidence: "*I think he would see it as a joke... I can't imagine he'd be easily deceived*", said one mother (Mother_2nd_Cycle_ESO_medium_SES); another added, "*I believe she has the wherewithal to consult us*", (Mother_2nd_Cycle_ESO_low_SES).

While Guerra and Taylor (2021) assert that susceptibility to scams does not solely depend on sociodemographic factors but also on individual and contextual factors, these observations suggest a pattern of vulnerability among different age groups. Notably, children are often depicted as the most vulnerable group, particularly when scams are perpetrated by influencers, seemingly trustworthy profiles (family or friends), or well-known brands. This vulnerability stems from their limited critical capacity and digital experience, underscoring the critical role of continuous parental supervision and early preventative digital education.

Conversely, secondary school students and older individuals, who have more extensive digital experience and frequent social media use, exhibit a more developed critical capacity. These adolescents quickly identify, evaluate, and dismiss the tactics of scams with a level of skepticism that often surpasses that of their parents (El-Asam and Katz, 2018). Hence, regular interaction with digital platforms, when coupled with parental involvement and preventive education, enhances the development of sophisticated critical skills essential for navigating online scams offering easy rewards.

5. Discussion and conclusions

This study provides insights into how adolescents and their parents perceive and respond to social media scams, underscoring the significant developmental and contextual factors that shape these dynamics. Our findings establish that, while younger adolescents rely heavily on parental guidance, the strategies employed—ranging from restrictive measures to trust-building approaches—directly influence the development of their critical capacities.

Adolescents' capacity to recognize scams evolves through exposure and familial dialogue. Younger participants, though curious and occasionally perceptive, often lack tools to independently identify deceptive schemes. This reliance on parents is consistent

with prior research (El-Asam and Katz, 2018; Shin and Kang, 2016), which emphasizes the necessity of adult intervention during the early developmental stages. However, restrictive approaches, while protective, may stifle the critical thinking needed for independent decision-making, as noted by Dedkova and Mýlek (2023). Our findings corroborate this limitation by suggesting the value of strategies that prioritize trust and open communication.

Parents in our study voiced varying levels of confidence in their children's critical skills, reflecting a tension between protective instincts and the recognition of growing adolescent autonomy. This tension highlights opportunities for reciprocal learning within families. Adolescents who actively engage in discussions about digital risks with their parents demonstrate greater resilience to scams, aligning with Wisniewski et al. (2025) and Cohen-Zilka (2017). Moreover, these conversations encourage adolescents to refine their skepticism and evaluative skills, creating a mutually reinforcing dynamic that benefits both the generations.

We observed a stark contrast in scam recognition across the age groups. Primary school children exhibit curiosity tempered by nascent skepticism, relying on parental cues to navigate online risks. Adolescents in secondary school displayed heightened critical awareness and readily identified scams through indicators, such as grammatical inconsistencies or implausible claims. In high school, many participants expressed frustration with peers or adults who fell victim to scams, reflecting their advanced evaluative capacity and internalization of preventive education.

This progression underscores the critical role that experience parents in fostering digital resilience. While younger adolescents benefit from direct guidance, older adolescents thrive when entrusted with greater autonomy and are equipped with tools to navigate risks independently. These observations resonate with theoretical frameworks such as

Steinberg's (2005) model of adolescent development, which links cognitive maturation to improved decision-making.

Parents' emotional intelligence emerged as a determining factor in effective mediation. As Mueller et al. (2020) asserted, emotionally intelligent parents better anticipate their children's vulnerabilities and foster environments conducive to open dialogue. This capacity not only strengthens familial trust, but also models critical behaviors that adolescents can emulate in digital contexts. Our findings extend this understanding by illustrating how emotionally attuned parenting bridges gaps between adolescent perception and reality, enhancing overall scam awareness.

This study contributes to the broader discourse on adolescent vulnerability to online fraud by focusing on scams offering "easy rewards". Unlike prior work centered on cyberbullying (Hong et al., 2025) or privacy breaches (El-Asam and Katz, 2018), our research illuminates how social engineering tactics exploit developmental and contextual vulnerabilities. By examining real-life interactions and familial dynamics, we provide a nuanced understanding of how adolescents internalize and apply critical thinking skills to counteract online threats.

Educational interventions should address the dual challenges of technical literacy and psychological resilience. Integrating scam recognition into school curricula could enhance adolescents' abilities to navigate deceptive content. These programs could benefit from incorporating scenario-based learning that mirrors real-world risks, as advocated by Christakis and Hale (2025). Simultaneously, parental training initiatives such as those proposed by Abdul-Morok et al. (2023) could empower families to collaboratively build defenses against digital fraud. The conceptual model in Figure 2 illustrates how scam awareness in adolescents results from a dynamic interplay between age-related development and parental mediation styles.

[Figure 2].

Ultimately, our exploratory findings confirm that digital resilience is a shared responsibility. Adolescents, parents, educators, and digital platforms must collectively adapt to the evolving online scamming landscape. Platforms, in particular, bear a significant responsibility for mitigating harm by minimizing dark patterns and increasing transparency. Meanwhile, families can act as frontline defenses, leveraging communication and mutual trust to safeguard against threats.

6. Recommendations, limitations and future lines of research

It is advisable for educational and governmental institutions to develop programs that equip adolescents with the skills to recognize fraudulent content from an early age, thereby fostering their development into critically aware adults. Moreover, enhancing the visibility of existing help or complaint lines targeted at young people would prove advantageous. In regions where such support mechanisms are absent, their establishment should be considered, especially on social media platforms.

In light of our findings and the theoretical grounding in social vulnerability and critical digital literacy, we propose an educational strategy that accounts for adolescents' developmental stage and socio-digital context: (a) for younger adolescents (11-13) who remain highly dependent on adult mediation and operate within concrete operational thinking, curricula should introduce foundational scam-awareness tools. These include identifying surface-level inconsistencies (e.g. usernames, logos, spelling), understanding why digital offers may be deceptive, and reinforcing adult consultation as a first response strategy; (b) for middle adolescents (14-15) who begin to internalize social heuristics and persuasive cues, programs should incorporate scenario-based activities that deconstruct manipulation tactics such as urgency, reciprocity, or false authority, which are techniques exploited in scams; and (c) for older adolescents (16-17)

who show increasing autonomy and critical reasoning, advanced modules should foster peer-led evaluation of scam content, critical reflection on influencer-driven marketing, and ethical analysis of platform dynamics. These interventions could advocate developmentally responsive digital resilience (Livingstone and Stoilova, 2021; Cohen-Zilka, 2017).

Influencer culture complicates the detection of scams among adolescents. Participants aged 11-15 cited influencers as trusted figures, often judging credibility through aesthetics, follower counts, and platform visibility. They rarely questioned promotional content when it appeared to be familiar or professionally produced. These observations align with persuasion literature that identifies adolescents' reliance on peripheral cues for critical evaluation (Hudders et al., 2017; Cohen-Zilka, 2017). Platforms should not treat disclosure compliance sufficiently. They must introduce stricter design policies to reduce scam-like exposure among minors, such as limiting reward-based claims in verified accounts targeting youth, filtering financial incentives embedded in entertainment content, and flagging posts that mimic known scam phrasing (e.g. "limited offer", "urgent", or "gift"). These design choices mirror the scam typologies that our participants failed to recognize. At the household level, adolescents who engage in open digital conversations with their parents demonstrate a stronger resistance to deceptive offers. Dialogic mediation, rather than punitive oversight, fosters the interpretive confidence that adolescents need to assess confident and persuasive content.

The study's limitations highlight the absence of a targeted focus on online scams, as these issues were analyzed within the broader context of challenges associated with young people's digital navigation. To address this, future investigations should delve into how preadolescents and adolescents perceive and respond to scams, with an emphasis on their developmental stages. For instance, preadolescents rely heavily on external guidance because of their emerging critical thinking skills, whereas older

adolescents exhibit more independent evaluative capacity. A more detailed understanding of these differences would allow scholars to better identify the vulnerabilities and protective factors specific to each subgroup within the broader population of young digital users.

Additionally, while the adopted qualitative approach provides valuable insights into participants' lived experiences, it inherently limits the generalizability of the findings. Incorporating mixed-methods, especially quantitative methods, would not only broaden the scope of these insights, but also enable comparisons across larger populations. Such approaches would be particularly valuable for highlighting age-specific trends and enhancing the applicability of conclusions to diverse contexts.

Moreover, the study's wide age range (11-17 years) encompasses significant developmental variability in cognitive, emotional, and social capacities, which influences how participants perceive risks and engage with digital environments. Although this diversity enriches the findings, the uniform application of the research questions across all participants introduces a limitation. Preadolescents (11-13 years) often depend more on external support systems, whereas adolescents (14-17 years) demonstrate greater autonomy in decision-making. Narrowing age brackets and tailoring research questions to these groups would yield more nuanced insights into the developmental trajectories that shape digital risk perception and responses to scams.

Finally, extending the scope of inquiry to include parents' perceptions of their children's critical capacities and their familiarity with reporting and remediation systems could provide a more comprehensive understanding of the intergenerational dynamics. While scams often target younger users, parents themselves may fall victim to fraudulent schemes, underscoring the need for studies exploring how these risks affect families as a whole. Furthermore, examining the appeal of low-effort rewards for younger users could inform the development of targeted interventions and early warning systems. By

addressing these dimensions, researchers can offer more robust strategies to mitigate online scams and enhance digital resilience across different age groups.

References

R. Abayomi-Aborisade, 2022. "Internet scamming and the techniques of neutralization: Parents' excuses and justifications for children's involvement in online dating fraud in Nigeria," *International Annals of Criminology,* volume 60, pp. 199-219. doi: https://doi.org/10.1017/cri.2022.13, accessed 10 May 2024.

N.N. Abdul-Morok, N.A.H. Abdul-Hakim, and N. Syazwani-Jamaludin, 2023. "SmartParents: Empowering parents to protect children from cyber threats," *International Journal on Perceptive and Cognitive Computing,* volume 9, number 2, pp. 73-79. doi: https://doi.org/10.31436/ijpcc.v9i2.406, accessed 9 May 2024.

A. Akdeniz-Kudubes, and Y. Sezer-Efe, 2023. "The predictive power of game addiction and social media addiction on adolescents' lifestyle," *Psychology in the Schools,* volume 61, number 3, pp. 1000-1017. doi: https://doi.org/10.1002/pits.23096, accessed 9 May 2024.

B. Andrino, D. Grasso, K. Llaneras and A. Sánchez, 2021. "El mapa de la renta de los españoles calle a calle [The income map of Spaniards street by street]" (30 April), at https://bit.ly/3JpRVi0, accessed 9 May 2024.

J. Bartlett, and C. Miller, 2011. *Truth, lies and the Internet. A report into young people's digital fluency.* London: DEMOS.

K. Boone, D. Babinski, A. Kujawa, S. Pegg, and C. Sharp, 2025. "The incremental validity of level of personality functioning over borderline personality features in associations with early adolescent social reward processing," *Personal Mental Health,* volume 19, number 1. doi: https://doi.org/10.1002/pmh.70000, accessed 9 January 2025.

M. Button, and C. Cross, 2017. “Technology and fraud: The “fraudogenic” consequences of the Internet revolution.” In: M. R. McGuire and T. Holt (editors), *The Routledge Handbook of technology, crime and justice*. London: Routledge, pp. 78-95. doi: https://doi.org/10.4324/9781315743981-5, accessed 10 May 2024.

D. Ceroni. and Y. Matthew. 2024. “Influence of Childhood Maltreatment on Machiavellianism.” *Journal of Aggression, Maltreatment & Trauma* 33(9): 1045–1054. https://doi.org/10.1080/10926771.2024.2358870, accesed May 2025

V. Chang, L. Golightly, X. Qianwen-Ariel, T. Boonmee, and B.S. Liu, 2023. “Cybersecurity for children: An investigation into the application of social media,” *Enterprise Information Systems,* volume 17, number 11, pp. 1496-1525. doi: https://doi.org/10.1080/17517575.2023.2188122, accessed 9 May 2024.

K. Charmaz, 2014. *Constructing grounded theory*. Los Angeles: SAGE Publications Inc.

D.A. Christakis, and L. Hale, 2025. *Handbook of children and screens. Digital media, development, and well-being from birth through adolescence.* Cham: Springer. doi: https://doi.org/10.1007/978-3-031-69362-5, accessed 7 January 2025.

G. Cohen-Zilka, 2017. “Awareness of eSafety and potential online dangers among children and teenagers,” *Journal of Information Technology Education,* volume 16, pp. 319-338. doi: https://doi.org/10.28945/3683, accessed 8 May 2024.

J. Corbin, and A. Strauss, 2008. *Basics of qualitative research: Techniques and procedures for developing grounded theory.* Los Angeles: SAGE Publications Inc.

C. Cross, and R. Layt, 2022. “‘I suspect that the pictures are stolen’: Romance fraud, identity crime, and responding to suspicious of inauthentic identities,” *Social*

Science Computer Review, volume 40, number 4, pp. 955-973. doi: https://doi.org/10.1177/0894439321999311, accessed 9 May 2024.

L. Dedkova, and V. Mýlek, 2023. "Parental mediation of online interactions and its relation to adolescents' contacts with new people online: the role of risk perception," *Information, Communication & Society,* volume 26, number 16, pp. 3179-3196. doi: https://doi.org/10.1080/1369118X.2022.2146985, accessed 9 January 2025.

E. Demurie, H. Van de Vyver, E. Sonuga-Barke, and H. Roeyers, 2025. "Age-related differences in temporal discounting of different types of reward," *Journal of Applied Developmental Psychology*, volume 97. doi: https://doi.org/10.1016/j.appdev.2024.101751, accessed 9 January 2025.

M. Dorasamy, M. Kaliannan, M. Jambulingam, I. Ramadhan, and A. Sivaji, 2021. "Parents' awareness on online predators: Cyber grooming deterrence," *The Qualitative Report,* volume 26, number 11, pp. 3683-3723. doi: https://doi.org/10.46743/2160-3715/2021.4914, accessed 10 May 2024.

A. El-Asam, and A. Katz, 2018. "Vulnerable young people and their experience of online risks." *Human-Computer Interaction,* volume 33, number 4, pp. 281-304. doi: https://doi.org/10.1080/07370024.2018.1437544, accessed 10 May 2024.

P. Fam, J. Yuin, M. Niko, J. Rumaya, and K. Maria, 2023. "Is parental mediation negatively associated with problematic media use among children and adolescents? A systematic review and meta-analysis," *Canadian Journal of Behavioural Science,* volume 55, number 2, pp. 89-99. doi: https://doi.org/10.1037/cbs0000320, accessed 9 January 2025.

B. Feijoo, E. Fernández-Gómez, and C. Sádaba, 2021. "Mobile as the new playground. Comparison of the consumption perception of YouTube and video games between

Chilean minors and their parents," *Prisma Social,* volume 34, pp. 146-164. https://bit.ly/3WSL22S, accessed 9 May 2024.

C. Feixa, 2011. "Past and present of adolescence in society: The 'teen brain' debate in perspective," *Neuroscience and Biobehavioral Reviews,* volume 35, pp. 1634-1543. doi: https://doi.org/10.1016/j.neubiorev.2011.02.013, accessed 7 January 2025.

C. Garitaonandia, I. Karrera-Xuarros, E. Jiménez-Iglesias, and N. Larrañaga, 2020. "Connected minors and online risks: Inappropriate content, inappropriate use of information, and excessive use of the Internet," *Profesional de la Información,* volume 29, number 4, pp. 1-10. doi: https://doi.org/10.3145/epi.2020.jul.36, accessed 8 May 2024.

Group-IB, 2022. *The Global State of Scams Report*. Group-IB. https://bit.ly/44NJmcZ, accessed 8 May 2024.

A. Guerra, and K. Taylor, 2021. "Scam susceptibility: Determining the dominant factor for an adolescent's decision making," *Journal of Student Research,* volume 10, number 4, pp. 1-16. doi: https://doi.org/10.47611/jsrhs.v10i4.1938, accessed 7 January, 2025.

J. Hong, 2012. "The state of phising attacks," *Communications of the ACM,* volume 55, number 1, pp. 74-81. doi: https://doi.org/10.1145/2063176.2063197, accessed 10 May 2024.

J.S. Hong, R. Navarro, and M.F. Wright, 2025. "Adolescent cyberbullying: A worldwide concern." In: *Encyclopedia of information science and technology*. New York, IGI Global, doi: https://doi.org/10.4018/978-1-6684-7366-5.ch017, accessed 8 January 2025.

L. Hudders, P. De Pauw, V. Cauberghe, K. Panic, B. Zarouali,, and E. Rozendaal, 2017. "Shedding New Light on How Advertising Literacy Can Affect Children's

Processing of Embedded Advertising Formats: A Future Research Agenda", *Journal of Advertising*, volume 46, number. 2, pp. 333–349. https://doi.org/10.1080/00913367.2016.1269303

T.N. Jagatic, N.A. Johnson, M. Jakobsson, and F. Menczer, 2007. "Social phising," *Communications of the ACM,* volume 50, number 10, pp. 94-100.

J. Jerrim. 2023. "Who Responds to Phishing Emails? An International Investigation of 15-Year-Olds Using PISA Data." *British Journal of Educational Studies* 71(6): 701–724 https://doi.org/10.1080/00071005.2023.2234456, accesed May 2025

H.S., Jones, J.N. Towse, N. Race, and T. Harrison, 2019. "Email fraud: The search for psychological predictors of susceptibility," *PloS One,* volume 14, number 1. doi: https://doi.org/10.1371/journal.pone.0209684, accessed 8 May 2024.

T. Kollmer, and A. Eckhardt, 2023. "Dark patterns. Conceptualization and future research directions," *Business & Information Systems Engineering,* volume 65, pp. 201-208. doi: https://doi.org/10.1007/s12599-022-00783-7, accessed 9 January 2025.

Pew Research Center, 2024. *How teens and parents approach screen time*: https://bit.ly/3DNPfxs, accessed 9 January 2025.

M. Landry, M. Turner, A. Vyas, and S. Wood, 2017. "Social media and sexual behavior among adolescents: Is there a link?," *JMIR Public Health Surveillance,* volume 3, number 2, p. e28. doi: https://doi.org/10.2196/publichealth.7149, accessed 9 May 2024.

A. Lareki, J.I. Martínez-de-Moretin, J. Altuna, and N. Amenabar, 2017. "Teenagers' perception of risk behaviors regarding digital technologies," *Computers in Human Behavior,* volume 68, pp. 395-402. doi: https://doi.org/10.1016/j.chb.2016.12.004, accessed 9 May 2024.

S. Livingstone, and M. Stoilova, 2021. "*The 4Cs: Classifying online risk to children.*" CO:RE – Children Online: Research and Evidence. doi: https://doi.org/10.21241/ssoar.71817, accessed 10 May 2024.

C. Miller, and J. Bartlett, 2012. "'Digital fluency': Towards young people's critical use of the Internet," *Journal of Information Literacy,* volume 6, number 2, pp. 35-55.

Ministry of the Interior. 2023. *Cybercrime Report in Spain 2023*. Madrid: Ministry of the Interior. Accessed May 22, 2025. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe-Cibercriminalidad_2023_126200212_pdfWEB.pdf

E.A. Mueller, S. Wood, Y. Hanoch, Y. Huang, and C.L. Reed, 2020. "Older and wiser: Age differences in susceptibility to investment fraud: The protective role of emotional intelligence," *Journal of Elder Abuse & Neglect,* volume 32, number 2, pp. 152-172. doi: https://doi.org/10.1080/08946566.2020.1736704, accessed 9 May 2024.

K. Muir, and A. Joinson, 2020. "An exploratory study into the negotiation of cyber-security within the family home," *Frontiers in Psychology,* volume 11, p. 424. doi: https://doi.org/10.3389/fpsyg.2020.00424, accessed 9 May 2024.

M. Nemilentseva, A. Tariq, W. Tariq, D. Aghajani, and M. Torkkeli, 2024. "A review of digital platform and circular economy. Opportunities and challenges for developing countries". In: *Human perspectives of industry 4.0 organizations. Reviewing sustainable performance,* Taylor & Francis Group. doi: https://doi.org/10.1201/9781032616810, accessed 8 January 2025.

Ohu, Francis C., and Lauren A. Jones. 2025. “The Intersection of Cyberwarfare, Social Media, and Adolescent Self-Esteem: A Forensic Cyberpsychology Analysis.” Paper presented at the *International Conference on Cyberwarfare and Security (ICCWS).*

M. O’Reilly, 2020. “Social media and adolescent mental health: The good, the bad and the ugly,” *Journal of Mental Health,* volume 29, number 2, pp. 200-206. doi: https://doi.org/10.1080/09638237.2020.1714007, accessed 10 May 2024.

Y.F. Paat, and C. Markham, 2021. “Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century,” *Social Work in Mental Health,* volume 19, number 1, pp. 18-40. doi: https://doi.org/10.1080/15332985.2020.1845281, accessed 9 May 2024.

K. Parti, 2023. “What is a capable guardian to older fraud victims? Comparison of younger and older victims’ characteristics of online fraud utilizing routine activity theory,” *Frontiers in Psychology,* volume 14, pp. 1-16. doi: https://doi.org/10.3389/fpsyg.2023.1118741, accessed 10 May 2024.

T. Piliouras, S, Crasto, C, Dharap, N, Gupta, and P, Yu,. 2025. “*Teaching Students Essential Survival Skills in the Age of Generative Artificial Intelligence: Critical Thinking, Digital Literacy, and Cybersecurity Awareness*.” Paper presented at the *2025 Northeast Section Conference*, March.

F. Quayyum, D.S. Cruzes, and L. Jaccheri, 2021. “Cybersecurity awareness for children: A systematic literature review,” *International Journal of Child-Computer Interaction,* volume 30, pp. 1-25. doi: https://doi.org/10.1016/j.ijcci.2021.100343, accessed 8 May 2024.

J. Salazar, I.T. Isabella, J.V. Maldonado, L. Hernandez, V.N. Bermudez, L.M. Acevedo-Farag, A.S. Bustamante, 2025. “Sustaining latine families’ cultural values through

technology mediation practices," *Journal of Latinos and Education*. doi: https://doi.org/10.1080/15348431.2024.2444942, accessed 9 January 2025.

J. Saul, R.F. Rodgers, and M. Saul, 2022. "Adolescent eating disorder risk and the social online world: An update," *Child & Adolescent Psychiatric Clinics,* volume 31, number 1, pp. 167-177. doi: https://doi.org/10.1016/j.chc.2021.09.004, accessed 9 May 2024.

Y. Sela, H. Omer, M. Mishali, and Y. Amichai-Hamburger, 2025. "The effectiveness of a novel parental training program in reducing problematic internet use of adolescents," *Journal of Family Psychology*. doi: https://doi/10.1037/fam0001285, accessed 9 January 2025.

W. Shin, and H. Kang, 2016. "Adolescents' privacy concerns and information disclosure online: The role of parents and the internet," *Computers in Human Behavior,* volume 54, pp. 114-123. doi: https://doi.org/10.1016/j.chb.2015.07.062, accessed 9 May 2024.

A. Soyoof, B.L. Reynolds, M. Neumann, J. Scull, E. Tour, and K. McLay, 2024. "The impact of parent mediation on young children's home digital literacy practices and learning: A narrative review," *Journal of Computer Assisted Learning,* volume 40, pp. 65-88. doi: https://doi.org/10.1111/jcal.12866, accessed 8 May 2024.

G. Stanley-Hall, 1904. *Adolescence – Its psychological and its relations to physiology, anthropology, sociology, sex, crime, and religion*. New York: Appleton.

J.M. Tanner, 1973. "Growing up," *Sci. Am*., volume 229, pp. 35-42, accessed 7 January 2025.

T. Vente, M. Daley, E. Killmeyer, and L.K. Grubb, 2020. "Association of social media use and high-risk behaviors in adolescents: Cross-sectional study," *JMIR*

Pediatrics and Parenting, volume 3, number 1. doi: https://doi.org/10.2196/18043, accessed 9 January 2025.

M.T. Whitty, 2013. "The Internet and its implications for children, parents and family relationships." In: A. Abela and J. Walker (editors), *Contemporary issues in family studies: Global perspectives on partnerships, parenting and support in a changing world*. Chichester: Wiley Online Library, pp. 262-274. doi: https://doi.org/10.1002/9781118320990.ch18, accessed 9 May 2024.

P. Wisniewski, H. Xu, M.B. Rosson, D.F. Perkins, and J.M. Carroll, 2016. "Dear diary: Teens reflect on their weekly online risk experiences." In: *CHI '16, Proceedings of the 2016 CHI conference on human factors in computing systems*. New York: Association for Computing Machinery, pp. 3919-3930. doi: https://doi.org/10.1145/2858036.2858317, accessed 9 May 2024.

P. Wisniewski, J. Park, K. Badillo-Urquiola, J. Gabrielli, J.L. Doty, and H. Hartikainen, 2025. "Moving beyond fear and restriction to promoting adolescent resilience and intentional technology use." In: Christakis, D.A., Hale, L. (eds) *Handbook of children and screens. Digital media, development, and well-being from birth through adolescence*. Cham: Springer, doi: https://doi.org/10.1007/978-3-031-69362-5_55, accessed 9 January 2025.

M. Workman, 2008. "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security," *Journal of the American Society for Information Science and Technology,* volume 59, number 4, p. 662e674. doi: https://doi.org/10.1002/asi.20779, accessed 10 May 2024.

Z. Xie, and Z. Duan, 2025. "Why did I fall for it? Exploring internet fraud susceptibility in the pig butchering scam," *Security Journal,* volume 38, number 9. doi: https://doi.org/10.1057/s41284-024-00457-x, accessed 8 January 2025.

TYPE OF SCAM	DESCRIPTION	EXAMPLE
Personal data verification scam	Scammers pretend to be trusted organizations and ask for personal details under false pretenses.	*An adolescent receives an email from a 'school portal' asking to verify login details.*
Identity theft	Scammers steal personal information and use it to impersonate the victim for fraud.	*An adolescent's stolen personal details are used to open fraudulent credit accounts.*
Deceptive reward schemes	Scammers promise a prize or special reward but require personal data or payment to claim it.	*An adolescent is told they won a free iPhone but must provide bank details to claim it.*
Advance fee fraud	Scammers ask for a small payment upfront, falsely promising a larger financial return.	*An adolescent is asked to send 50€ to receive a promised 500€ lottery prize.*
Romantic scam	Scammers build an emotional connection online to manipulate the victim into sending money.	*An adolescent is convinced by an online partner to send money for an emergency.*
Phishing (school-related)	Scammers send fake emails or messages that appear to be from a school to steal login credentials.	*An adolescent receives an email claiming their school account will be closed unless they enter credentials.*
Fake scholarship offers	Scammers advertise fake scholarship programs to collect personal and financial information.	*An adolescent applies for a fake scholarship and is asked to pay an application fee first.*
Bogus contests	Scammers create fake contests and trick victims into paying fees or sharing personal data.	*An adolescent participates in a fake contest on social media but never receives the prize.*
Gaming scam	Scammers offer discounted in-game purchases but take the payment without delivering the item.	*An adolescent buys in-game currency from an unofficial seller but never gets the items.*
Fraudulent subscription service	Scammers promote free trial services but secretly charge hidden fees or make cancellation difficult.	*An adolescent signs-up for a free trial but starts receiving unauthorized monthly charges.*
Counterfeit giveaways	Scammers advertise free gaming currency or prizes but require personal or payment details first.	*An adolescent finds a website offering free V-Bucks (for the Fornite game) but is asked to provide credit card details.*

Figure 1. Types of scams, descriptions, and examples. Created by the authors based on Guerra and Taylor (2021), Parti (2023), and Xie and Duan (2025).

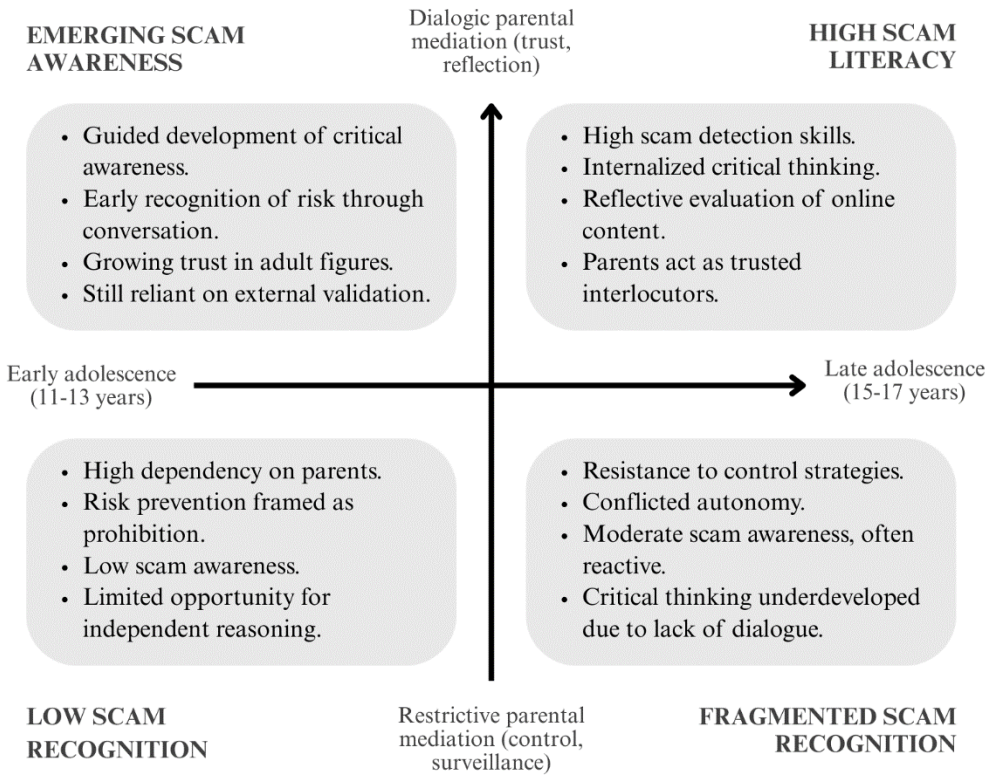

Figure 2. Conceptual model of the interaction between age, parental mediation style, and adolescents' scam awareness. Created by the authors.

Age	Spanish System		British System		American System	
11-12	Primary School	6th grade of primary	Key stage 3	Year 7	MIDDLE SCHOOL	6th Grade
12-13	1st cycle ESO	1º ESO		Year 8		7th Grade
13-14		2º ESO		Year 9		8th Grade
14-15	2nd cycle ESO	3º ESO	Key stage 4	Year 10		9th Grade
15-16		4º ESO		Year 11	HIGH SCHOOL	10th Grade
16-17	Baccalaureate	1º Baccalaureate	Key stage 5	Year 12		11th Grade
17-18		2º Baccalaureate		Year 13		12th Grade

Table 1. Equivalence of secondary education stages in Spain with those in other countries (UK and USA).

RQ	Interview questions (adolescents)	Interview questions (parents)
Perception of the spread of scams on social networks	Have you encountered scams on social networks? Have you fallen for any scams? If so, what did you do? Who did you turn to first: your family or your friends? How do you perceive your parents and teachers' familiarity with this topic? Do you discuss this type of content at home or at school?	One of the concerns that often worries parents is the dangers on the internet. What issues are they most concerned about? What is your opinion on social media scams?

	[After viewing the examples]	
Level of critical awareness of scams on social networks	What do you think is the source of this post? Where was it published? What is its message? What is the intent of this content? [After the questions, it is clarified that the content may be intended as a fraud.]	[After viewing the examples] Had you noticed posts of this kind on social networks before? Had you realized that this could be considered scam content?
Parental perception of adolescents' critical capacity regarding scams on social networks		Do you think your child would be able to detect these types of fraudulent practices?

Table 2. Summary of the interview guiding questions.