Online Fraud:

security challenges and preventive measures for accommodation platform users

Michal Radošinský[1], Saba Najjar[2] and Łukasz P. Wojciechowski[3]

Abstract

The text focuses on the development and impact of generative artificial intelligence (GenAI) in the context of online fraud and manipulation. The methodology applied is desk research, involving the analysis of existing studies, fraud cases, expert opinions, and comparative insights from platform practices. The findings highlight the growing sophistication of fraud mechanisms, supported by AI-generated content, and emphasize the importance of digital literacy, trust mechanisms, and technological countermeasures. It emphasizes that GenAI enables the creation of highly realistic fake profiles, images, and texts that are difficult to distinguish from authentic content. This capability presents a significant risk of loss of trust for online platforms such as social media, marketplaces, and travel agencies. Particular emphasis is placed on the importance of media literacy and fact-checking as key tools in combating misleading information. The study presents a set of recommendations to enhance user safety and calls for coordinated efforts between platform providers, users, and AI developers. The study analyzes sophisticated fraudster tactics, including fake advertisements and phishing sites that exploit travelers' trust.

Keywords

Artificial intelligence; Abuse and manipulation; Scams and phishing; Accommodation services; Cybersecurity.

[1] Assistant Professor at the University of SS. Cyril and Methodius in Trnava. E-mail: radosinsky1@ucm.sk.
[2] M. Arch., Tor Vergata University of Rome, saba. E-mail: najjar@students.uniroma2.eu.
[3] PhD, Associate Professor at the University of SS. Cyril and Methodius in Trnava. E-mail: lukasz.wojciechowski@ucm.sk.

LUMINA
Revista do Programa de Pós-graduação em Comunicação
Universidade Federal de Juiz de Fora / UFJF
e-ISSN 1981-4070

Fraude Online:

desafios de segurança e medidas preventivas para utilizadores de plataformas de alojamento

Michal Radošinský[1], Saba Najjar[2] e Łukasz P. Wojciechowski[3]

LUMINA
Revista do Programa de Pós-graduação em Comunicação
Universidade Federal de Juiz de Fora / UFJF
e-ISSN 1981-4070

Resumo

O texto foca no desenvolvimento e no impacto da inteligência artificial generativa (IAG) no contexto de fraudes e manipulações on-line. A metodologia aplicada é a pesquisa documental, envolvendo a análise de estudos existentes, casos de fraude, opiniões de especialistas e percepções comparativas das práticas das plataformas. Os resultados destacam a crescente sofisticação dos mecanismos de fraude, apoiados por conteúdos gerados por IA, e ressaltam a importância da alfabetização digital, dos mecanismos de confiança e das contramedidas tecnológicas. Salienta-se que a IAG possibilita a criação de perfis falsos, imagens e textos altamente realistas, difíceis de distinguir do conteúdo autêntico. Essa capacidade representa um risco significativo de perda de confiança em plataformas on-line, como redes sociais, marketplaces e agências de viagens. Dá-se ênfase especial à importância da alfabetização midiática e da checagem de fatos como ferramentas-chave no combate à desinformação. O estudo apresenta um conjunto de recomendações para aumentar a segurança dos usuários e defende esforços coordenados entre provedores de plataformas, usuários e desenvolvedores de IA. Também são analisadas táticas sofisticadas empregadas por fraudadores, incluindo anúncios falsos e sites de *phishing* que exploram a confiança dos viajantes.

Palavras-chave

Inteligência artificial; Abuso e manipulação; Golpes e phishing; Serviços de acomodação; Cibersegurança.

[1] Professor Assistente na Faculdade de Comunicação de Mídia da Universidade de São Cirilo e Metódio em Trnava, Eslováquia. Doutor em Metodologia da Língua e Literatura Inglesa. E-mail: radosinsky1@ucm.sk.

[2] Mestre em Arquitetura, Universidade Tor Vergata de Roma. E-mail: najjar@students.uniroma2.eu.

[3] Doutor, professor associado na Universidade de São Cirilo e Metódio em Trnava. E-mail: lukasz.wojciechowski@ucm.sk.

Introduction

Generative artificial intelligence (GenAI) has revolutionized digital platforms, but its misuse has opened avenues for fraud, particularly in the hospitality sector. This study explores these risks and offers actionable strategies for mitigating fraud. This pattern of technological behaviour is particularly important in the contemporary era of AI development.

The development of artificial intelligence has been ongoing for several decades, as evidenced by works such as Slagle's (1971). Scholarly discourse on AI's societal implications predates public awareness, as documented in comprehensive publications by Arbib and Trappl (1987). Academic institutions globally have been scrutinizing artificial intelligence's trajectory since the mid-second decade of the 21st century. Graves (2018) critically examines automated fact-verification's potential and constraints. The research investigates how technological advancements in natural language processing and machine learning can support journalistic and individual fact-checking efforts, facilitating disinformation detection. Graves acknowledges automated fact-checking's efficiency in resource optimization and expedited misinformation identification, while simultaneously highlighting critical technological limitations, including contextual comprehension deficits and inherent vulnerability to manipulation strategies (Graves, 2018). Automated fact-checking itself is faster and often cheaper for companies. However, it does not fully replace human judgment.

Contemporary technological ecosystems represent the culmination of extensive developmental trajectories. Harold Cohen's AARON software, for instance, served as a prototype for generative platforms like Leonardo.ai. This proto-software constitutes a computational framework capable of generating original artistic representations. Cohen initiated AARON's development in 1972, continuing until he died in 2016. Unlike contemporary AI models, AARON lacked autonomous learning capabilities, requiring manual programming for each novel functionality. Nevertheless, the software demonstrated remarkable generative potential, producing virtually infinite image variations within predefined stylistic parameters, presaging current GenAI technologies (Morbey, 1992).

Much of the public discourse on GenAI has, to date, been centered on ChatGPT, created by OpenAI in 2018 and released for public use in November 2022 (Marr, 2023). A generative model built on transformer architecture, ChatGPT uses deep-learning and machine-learning algorithms to produce conversational and humanlike text responses. GenAI chatbots are not a new concept, but ChatGPT does represent a watershed moment in the history of GenAI due to its superior mimicry of human-like conversations on a variety of topics that appear natural (Alawida *et al.*, 2024; OOI *et al.*, 2023) and there are not rare cases that end tragically with suicide because of love (Roose, 2024) when students spent several months interacting with chatbots on Character.AI. This role-playing platform enables users to design their own AI-powered characters or engage in conversations with characters created by others.

Nonetheless, risks associated with GenAI tools like ChatGPT have also been identified in terms of the manipulation of individual persons (Eliot, 2023). Due to its ability to generate convincing human-like texts and to propagate false information, GenAI may be used to influence or manipulate people'behavior, perceptions, and emotions (Wach *et al.*, 2023), which often accelerates dark creativity (Cropley *et al.*, 2010; Kapoor; Puthillam, 2024) as an opposition for positive creative productions (Fichnová, 2013) that are beneficial to humanity.

Methodology

In this paper, we employed the desk research method, also known as secondary research, utilizing existing data and information to gain insights on the given topic. It involves the collection and analysis of existing data or information that has already been published. The desk research method involves systematic collection, deduction and induction, analysis, and synthesis of existing data from various sources including academic literature, reports, popularization, and newspaper articles, and of course expert analyses. The aim of the study is to audit the current situation of fraud risks with a special focus on the impact of technologies and to present easily implementable strategies for platforms and users to increase security and trust. To achieve this goal, we followed these methodological steps:

1. Literature review: We conducted an extensive review of academic publications, reports, and credible public sources on the development of AI technologies, their applications in fraud detection, and emerging challenges in online security;

2. Presentation of specific studies: We examined reported fraud incidents on major platforms such as Airbnb and Booking.com to identify common patterns and tactics used by fraudsters;

3. Synthesis of expert opinions: We analyzed insights from cybersecurity experts and platform representatives to understand current best practices and future trends in fraud prevention;

4. Comparative analysis: We compared different approaches to fraud detection and prevention across various online platforms to identify the most effective strategies.

In the context of our study on GenAI and online fraud, desk research enabled us to synthesize information from diverse sources. (Kiely, 2024). The crucial advantage of this form of information gathering is the potential to quickly synthesize a wide range of information from heterogeneous sources, providing a comprehensive overview of the status quo. It is also correct to acknowledge that this approach has limitations, such as potential subjectivity in secondary data and a lack of primary data collection. To mitigate these limitations, we ensured the use of various reliable and current sources, cross-verifying information. This approach provided a comprehensive view of the development of AI technologies, their applications in fraud detection, and the emerging challenges in online security.

The Rise of Generative AI and Deepfakes

In today's rapidly evolving world, Deepfake images can easily be produced on websites such as Generated Photos, UnrealPerson.com, and ThisPersonDoesNotExist.com, which generate unique, extremely detailed, and life-like images of human bodies, torsos, and headshots. While such images do not represent a real person, they can potentially be used by bad actors in conjunction with aliases to publish inauthentic user profiles on any number of online platforms.

Users of Facebook, Instagram, and WhatsApp report losing vast sums of money, sometimes amounting to an individual's life savings, after being ensnared by fake investment advertisements or by fraudster impersonators via these platforms (Clark; Wood, 2023). Scammers publish fake profiles advertising their services as freelancers on hiring platforms such as Fiverr and Upwork, often offering low prices to entice buyers. Such scammers will direct their clients to pay upfront outside of secure payment portals via Venmo or other payment systems, subsequently disappearing with the money, and without delivering the services paid for (Cudd, 2022).

Recent studies have found that AI-generated faces are now largely indistinguishable from human faces (Miller *et al.*, 2023), and that AI-synthesised face images are routinely perceived to be more trustworthy than real ones (Nightingale; Farid, 2022). Facebook Marketplace allows sellers and buyers of consumer items to connect directly, without a "middleman." Scammers on the platform use various tactics of deception, which include the advertising of counterfeit, defective, or entirely fictitious items; fake giveaways constructed to steal confidential personal information; and forged payment receipts displaying a supposedly successful payment for an item (Shah, 2023). It is important to realize that in the online space, just like on the street, we are not completely safe and must be vigilant.

In addition, GenAI technologies now enable the creation of sophisticated synthetic content, including photorealistic imagery, abbreviated video segments, and concise audio recordings. Fraudsters can take data to train AI from real people to make their crimes more credible (Bürge, 2024). Materials are so easily accessible that they can steal anyone's identity. The most common frauds include stolen credit card information and bank details after entering information on a fake website, clicking on phishing links, or false photos. However, people are not sufficiently cautious. Everyone can defend themselves using free tools. One of the effective means available to everyone is reverse-image search (Key, 2024). Our sight and perception are not perfect, and we must be aware of this. If we don't have an experienced person nearby to help us with critical thinking, we are left with only online tools.

Unequivocally, the contemporary landscape of 2024 presents unprecedented challenges in digital information verification, particularly concerning GenAI and deepfake technologies. Fraudulent activities in the accommodation sector are becoming increasingly widespread and affect various online platforms. These scams are reported not only by the media and scientists but also by ordinary internet users who share their experiences and warn others about fraudulent practices. The scammers' procedure is relatively consistent. They first gain access to an existing account on platforms like Airbnb or create a completely new account with several fake reviews. They then search for real estate in the desired location and obtain photographic materials, either by stealing existing images from the internet or using artificial intelligence generators. Expanding on this in the next two sections, there will be a deeper look into how complex, yet possible, deception within homestays and GenAI fraud is.

Online Homestay Marketplace Platforms

Online homestay marketplace platforms, such as Airbnb and Booking.com, operate on a two-sided business model, connecting travelers with property owners. These platforms facilitate value creation by offering travelers diverse accommodation options while enabling hosts to reach a global audience. For instance, platforms like Airbnb and Booking.com dominate the online accommodation marketplace. These platforms have transformed the hospitality industry by providing a seamless digital interface for booking and managing stays, catering to millions of users worldwide. Airbnb, as the largest homestay marketplace, offers more rooms globally than the top five hotel chains combined. Similarly, Booking.com, with its extensive network of hotels, apartments, and vacation rentals, leads the market in diverse offerings, providing seamless booking experiences and catering to millions of travelers daily. Founded in 2007, Airbnb has grown to host over 8 million property listings as of June 2024, surpassing the combined capacity of the five largest hotel chains (Airbnb, 2024; Gallagher, 2018; Hartmans, 2017; Stone, 2018). Airbnb earns revenue by charging a flat commission from hosts for every booking made via the platform, as well as a percentage of the booking amount as a transaction fee on each confirmed booking (Walsh *et al.*, 2020). Host users produce property listings, reviews authored by host users and guest users, and sometimes they even provide a private messaging service similar to those found on social media apps such as Instagram or Facebook.

A vast gamut of studies has highlighted the vital role of trust in sharing accommodation platforms; thereby, the study proposes its inclusion under a separate category. Several studies have highlighted the critical role played by trust in P2P accommodation (Chatterjee *et al.*, 2019; Farmaki; Kaniadakis, 2020; Mao; Wei, 2019; Phua, 2018; Tussyadiah, 2015). Given the reliance of these platforms on trust-based interactions, understanding the mechanisms of user credibility and security remains crucial for sustaining their growth and reliability.

Trust and Fraud in the Sharing Economy

The proliferation of generative artificial intelligence introduces increasingly sophisticated online fraud mechanisms. Scammers can now fabricate hyper-realistic digital profiles, electronic communications, and photographic representations designed to manipulate digital platform users. Platforms like Airbnb, fundamentally predicated on interpersonal trust models, become particularly vulnerable to such technologically mediated fraudulent interventions (Reid, 2024). Large brands provide guarantees to their customers, thereby increasing comfort and attracting more and more customers.

Over time, online homestay platforms have grown by offering diverse accommodation options worldwide. However, not every booking goes smoothly. Beneath the surface of five-star reviews and polished photos, some guests have been caught in scams, ranging from inconvenient to downright terrifying. Without knowing the negative implications for guests, these scams include fake listings, surprise fees, and hosts who disappear at the last minute (Popov, 2024a). Therefore, one of the recommendations could be to ensure that we are on the correct official website of the platform.

Moreover, there is the foundation of the sharing economy, which is built on mutual trust between users and service providers. The business model of sharing-economy platforms would be unsustainable and unprofitable if the operators of these intermediary platforms were unable to convince the majority of users to trust the safety of the value exchange advertised on the platforms. In other words, to participate in the sharing economy, you must be willing to trust a stranger. Therefore, whether booking a stay or requesting a rideshare, participants must place significant trust in strangers. The user must also trust that the driver is not a criminal, a kidnapper, a rapist, or a murderer, which sadly has proven to sometimes be the case (Bensinger, 2019; Dent, 2022). If the user had reason to believe nefarious intent on the part of the driver, the user would not voluntarily enter the car nor hail the ride in the first place. The same reliance on the notion of trust applies to the business model of online homestay marketplace platforms because guest users are required to relocate themselves to a specified location and enter the home of a stranger.

Platform Security Measures and Their Limitations

Realizing that trust and safety are central to the sustainability and profitability of its business (Airbnb, 2022; Gebbia, 2016; Zamani *et al.*, 2019), these platforms have established several multilayer defense mechanisms against scams (Airbnb, 2022; Walsh *et al.*, 2020), including specialist emergency response teams to assist users when things do go wrong on the platform (Carville, 2021). Such measures have had varying success since scams still occur in the online hospitality sector (Conti, 2019; Fergusson, 2021), as scammers continually adapt to defenses and seek out new ways to fool the system (Ekstein, 2023). The emergence of generative AI (GenAI) has intensified the challenge of fraud detection and prevention. Previously, setting up a network of fake host profiles and fraudulent reviews required substantial time and effort. However, with GenAI, scammers can now generate fake listings, automated review bots, and highly convincing phishing emails within minutes, drastically expanding their reach. Even with advanced security measures, the rapid evolution of AI-driven fraud underscores the urgency for continuous innovation in fraud prevention strategies. The next phase of platform security will require collaborative efforts between AI developers, regulators, and platform operators to build fraud-resistant systems that evolve alongside generative AI advancements.

Our findings align with existing literature on GenAI-enhanced fraud (Reid, 2024; Popov, 2024a), and extend current discussions by providing user-centered preventive strategies. Trust mechanisms and digital literacy emerged as recurring themes, echoing prior studies (Zamani *et al.*, 2019; Walsh *et al.*, 2020). However, our study also identified a gap in comparative evaluations of platform security measures, which future primary research could explore in more depth.

Media Coverage and Public Education

The emergence and exponential development of artificial intelligence technologies simultaneously offer unprecedented research opportunities for comprehensively categorizing and analyzing touristic fraud typologies (Ding *et al.*, 2022). Beyond academic research, mainstream media platforms play a crucial role in public education, disseminating knowledge about fraud detection and prevention strategies.

In January 2024, The Guardian reported a critically problematic scenario involving fraudulent activities targeting Booking.com's accommodation partners. These malicious actors employed sophisticated phishing email strategies designed to compromise accommodation providers' computational systems. Through these strategies, they successfully illicitly acquired in excess of $337,000 from unsuspecting customers (BEAZLEY, 2024). The operational methodology involves initiating a transaction wherein after payment, fraudsters either completely vanish, leaving purchasers without accommodation, or attempt subsequent monetary extractions through manipulative communication techniques.

The BBC's summer reportage revealed alarming statistical data from Booking.com, documenting an unprecedented fraud proliferation ranging between 500-900% over an 18-month period (Gerken, 2024). The primary attribution for this exponential increase targets generative artificial intelligence tools like ChatGPT, which facilitate rapid, large-scale production of sophisticated fraudulent electronic communications. These communications strategically aim to manipulate recipients into divulging personal information through fabricated online reservation hyperlinks. Primary targets include prominent platforms such as Booking.com and Airbnb. The BBC's analytical investigation of fraudulent activities in the online accommodation sector reveals a long-standing negative phenomenon.

Despite the presence of evident fraudulent communication indicators — manifesting through linguistic irregularities and grammatical anomalies — a significant user demographic demonstrates insufficient interpretative diligence. A critical systemic deficiency persists: the pronounced absence of proactive reporting of fraudulent activity to the Booking.com platform by affected users. This reporting passivity enables fraud perpetrators to continuously operate through singular user profiles, exponentially increasing potential financial fraud victim populations (BBC London, 2023). From a pragmatic perspective, however, we must state that the online world is a reflection of the physical world. Therefore, as a certain part of the population has moved online, fraudulent activities have inevitably moved there as well.

To further illustrate a real world case, Marnie Wilking, serving as Chief Information Security Officer at Booking.com, presented groundbreaking cybersecurity findings at a conference. Her comprehensive analysis posits that phishing attacks represent a persistent security challenge, evolutionarily paralleling electronic communication's developmental trajectory. A significant qualitative and quantitative attack escalation was documented following the implementation of the advanced artificial intelligence system in 2022. Artificial intelligence technologies provided malevolent digital actors with unprecedented sophisticated tools for generating fraudulent multilingual communications at scale. In a strategic response, Booking.com implemented proprietary AI solutions designed to detect and in minutes eliminate fraudulent hospitality offerings, fundamentally aimed at consumer protection against potential fraudulent activities (Why [...], 2024).

As we can see, the ongoing arms race between cybercriminals and security experts underscores the critical need for continuous innovation in AI-powered defense mechanisms. We are approaching a time when our human senses will not be able to discern what is true and what is false, and therefore, we must rely on technology that will protect us.

Education and Prevention Strategies

Another way to prevent such atrocities from happening is educating oneself. Fact-checking is also a special tool for the development of media competencies in the process of media education. Media literacy and their phenomena is considered to be one of the core educational mechanisms of "immunization" against fake news, and an activator of the critical approach, preventing their occurrence (Kačinová, 2022). The problem with such information in the form of circulating fake news or some groups of hoaxes lies in the distortion or manipulation of reality, as well as the recipient's perception and evaluation of reality.

Fortunately, numerous researchers and scientific professionals are actively engaged in educational initiatives designed to cultivate digital vigilance within this emergent artificial intelligence ecosystem. Fraudulent activities represent substantial financial risk vectors, not merely for individual economic agents but also for institutional and governmental entities. Baweja *et al.* (2023) propose a system for increasing awareness about investment fraud that utilizes machine learning and gamification techniques to educate people in this area. This system, based on machine learning, can personalize education for each user. It uses a knowledge base created by experts, from which it selects information about specific frauds for each user. (Baweja *et al.*, 2023) By bridging the gap between technological innovation and user education, such approaches aim to create more resilient and informed digital citizens. A fraudulent offer is often more tempting than a real one.

A common strategy involves creating realistic but fraudulent property listings on trusted platforms or designing fake booking websites that mimic legitimate ones. Scammers frequently lure victims with deals that seem too good to be true. Upon engagement, travelers are redirected to unofficial payment channels or phishing sites, leading to stolen funds or compromised personal data. Research highlights how scammers exploit vulnerabilities in both peer-to-peer platforms and hotel booking systems, often targeting travelers' urgency and unfamiliarity with local norms (Popov, 2024b; Souček; Jizba, 2024).

An appropriate prevention is understanding how internet frauds work and learning to resist the temptation of immediate monetary benefits. Financially impulsive individuals often do not consider the risks of financial loss, and this recklessness increases the chances of becoming a victim of online fraud. Internet users tend to ignore privacy protection risks until they personally encounter online fraud (Chen *et al.*, 2017). Generative AI tools can identify fraudulent behaviors through anomaly detection, real-time analysis, and natural language processing. These technologies not only detect scams but also predict potential fraud patterns.

Fraud Detection and Recommendations

To understand the application of artificial intelligence models in online fraud detection between 2019 and 2024, a systematic literature review was comprehensively conducted. The research identified sixteen distinct fraud typologies and analyzed contemporary natural language processing techniques employed in fraudulent activity detection. The study revealed significant methodological limitations, particularly regarding generalizability. Existing models predominantly exhibit a narrow focus, concentrating on specific fraud manifestations while demonstrating restricted effectiveness against the rapidly evolving landscape of fraudulent activities. Additional critical challenges include selective performance metric reporting and insufficient model transparency.

An emerging technological trend involves the increasingly sophisticated deployment of advanced AI systems like ChatGPT, which paradoxically serve dual functions—potentially generating fraudulent content while simultaneously providing countermeasure strategies (Papasavva *et al.*, 2024). Leveraging AI-driven fraud detection tools, including anomaly detection algorithms and real-time phishing detection systems, can significantly reduce risks for both platforms and users.

Such fraudulent offers allow accommodation bookings several months in advance, requiring a reservation fee that cannot be refunded (Financial Life, 2022). To avoid becoming a victim of fraud, we recommend several preventive steps:

1. Before booking, contact the host and verify their communication ability. Simply ask a few ordinary questions.

2. Check the cancellation conditions. The inability to cancel does not automatically mean fraud, but it can be a warning sign.

3. Verify the host's identity – confirm that they are actually from the location of the accommodation.

4. Check the accommodation's history – whether it has been previously booked and what genuine reviews it has.

5. After booking, send an email to the host through the Airbnb platform, then call the provided phone number and verify its functionality.

6. Check whether the property is currently for sale or was recently sold. In such a case, contact the relevant real estate agent.

7. If possible, verify the information through someone who personally knows the location.

8. Checking URLs for authenticity—looking for 'https' and a padlock icon—helps users differentiate legitimate websites from imposters.

9. Avoiding unsolicited links in emails or advertisements and instead navigating directly to the platform reduces phishing risks (SouČek *et al.*, 2024).

10. Conduct all transactions and communications within verified platforms

for added security.

11. Avoid unsolicited links in emails or ads; instead, navigate directly to the platform to reduce phishing risks.

12. Use reverse image search to verify property photos and ensure they are not stolen from other listings or websites.

When shopping online, be extremely cautious, such as checking the seller's reputation before purchasing and being wary of offers that seem too cheap to be true (Balakrishnan; Bakar, 2024). Critical evaluation of unusually low-priced deals by cross-checking prices on reputable platforms and reading customer reviews can help validate a property's legitimacy. Secure payment methods, such as credit cards, also offer protection, allowing for disputes in case of fraud. Combining these strategies with platform-specific protections, like Airbnb's Guest Refund Policy, can significantly reduce exposure to scams (Popov, 2024a). In the context of online booking platforms, reviews and ratings play a significant role in shaping trust perception. Feedback from our colleagues or acquaintances is also important (Christin, Nugraha, 2023).

Accommodation scams may maintain a similar structure to the past, but thanks to artificial intelligence technologies, they are now much more sophisticated and convincing.

Limitations and Future Works

This study relied primarily on desk research, which has some inherent limitations, such as the potential for bias in secondary data and the lack of direct input from primary sources. While secondary data can provide valuable context, it may not fully capture the dynamic nature of real-world situations. To mitigate this, the research utilized a variety of reliable sources, including peer-reviewed journals, industry reports, and expert analyses, ensuring a comprehensive and well-rounded understanding.

However, future studies should address these limitations by incorporating more direct data collection methods, such as surveys, interviews, or case studies. These would allow for a deeper exploration of user behavior, platform vulnerabilities, and the evolving tactics of fraudsters. Moreover, collaboration among AI developers, platform operators, regulatory bodies, and users is crucial for developing robust, scalable fraud prevention systems. This should include greater transparency, consistent standards across platforms, and ongoing efforts in digital literacy education. By tackling these challenges, we can ensure that emerging technologies like generative AI are used responsibly and effectively to combat fraud in the online hospitality industry.

Discussion

Through analysis of available literature and published fraud cases, we've found that fake accommodation scams are a long-standing problem. We gathered data from investigative reports that aim to educate the general public in an accessible way while providing valuable information about the phases, tools, and outcomes of accommodation fraud. Artificial intelligence, however, makes these scams much more sophisticated and helps scammers automate this process. Besides pointing out tools for detecting fraudulent texts and photos, we've collected simple, classic advice on how to protect yourself effectively. In conclusion, we recommend being vigilant, researching information in advance, checking the location on Google Street View, verifying as much information as possible, and not relying solely on platform protection mechanisms. Although in many cases you may get your money back for fraudulent accommodation, you can save yourself from unnecessary stress. Remember, if you end up on the street without accommodation and have to quickly find alternative lodging, it's often several times more expensive than the original booking. Your vacation can become more costly and filled with negative emotions.

Conclusion

This study has highlighted how online fraud within the accommodation sector, particularly as facilitated by generative artificial intelligence (GenAI), is growing. Through extensive desk research — exploring into peer-reviewed studies, media investigations, expert commentaries, and platform reports — we examined how scammers utilize GenAI to generate remarkably compelling fake profiles, property listings, and phishing communicat. These tactics are continuously circumventing standard detection practices and are creating risk for the fundamental trust that peer-to-peer hospitality platforms are built on.

Our findings show that technology alone is not a sufficient answer. While detection systems powered by AI are developing, alertness on the part of the user is still one of the best lines of defense. This study adds to the literature by merging technological and behavioral perspectives, illustrating that the enhancement of digital literacy is just as important, if not more so, than improving the security protocols of given platforms. Our findings were compared with previous studies, such as Zamani *et al.* (2019) and Walsh *et al.* (2020), as we highlighted the centrality of trust-building in sustaining user engagement and safety. Nonetheless, our analysis also uncovers a lack of coverage in the literature—especially regarding users' credibility evaluation in AI-mediated spaces—which should inform future experiential work.

In practice, we advise platforms to take transparent and collaborative approaches, with cybersecurity experts and regulators working together on scalable prevention measures. Users, in turn, must be provided continuous educational tools in the form of tutorials, alert systems, and fact-checkers. From a research perspective, future work should focus on mixed-method studies that combine platform data with user interviews and behavioral experiments. This will allow for further understanding and awareness on the nature of digital-fraud and how individuals and institutions can stay resilient.

Artigo submetido em 21/12/2024 e aceito em 25/04/2025.

References

AIRBNB. Airbnb fast facts. **Airbnb Newsroom**, [*s.l.*], 1 ago. 2024. Disponível em: https://shorturl.at/UoHzc. Acesso em: 1 ago. 2024.

AIRBNB. Airbnb launches the Trust and Safety Advisory Coalition. **Airbnb Newsroom**, [*s.l.*], 13 maio 2022. Disponível em: https://shorturl.at/1EodN. Acesso em: 18 nov. 2024.

ALAWIDA, M.; SHAWAR, B. A.; ABIODUN, O. I.; MEHMOOD, A.; OMOLARA, A. E.; AL HWAITAT, A. K. Unveiling the dark side of ChatGPT: Exploring cyberattacks and enhancing user awareness. **Information**, v. 15, n. 1, p. 1–26, 2024. DOI: https://doi.org/10.3390/info15010027.

ARBIB, M. A.; TRAPPL, R. **Impacts of artificial intelligence**: scientific, technological, military, economic, societal, cultural, and political. North-Holland, 1987.

BALAKRISHNAN, T.; BAKAR, E. A. Factors that Enhance Consumer Self-Protection Against Online Shopping Scams. **International Journal of Academic Research in Business and Social Sciences**, v. 14, n. 10, p. 2088-2097, 2024. DOI: http://dx.doi.org/10.6007/IJARBSS/v14-i10/23323.

BAWEJA, P.; SANGPETCH, O.; SANGPETCH, A. AI For Fraud Awareness. **arXiv**, [*s.l.*], 2023. DOI: https://doi.org/10.48550/arXiv.2308.11032.

BEAZLEY, J. Booking.com scams surge 580% with hundreds of thousands of dollars in losses, ACCC says. **The Guardian**, [*s.l.*], 31 jan. 2024. Disponível em: https://shorturl.at/CeoO9. Acesso em: 19 nov. 2024.

BENSINGER, G. When rides go wrong: How Uber's investigations unit works to limit the company's liability. **The Washington Post**, 26 set. 2019. Disponível em: https://shorturl.at/xkHOS. Acesso em: 18 nov. 2024.

BOOKING.COM scam. **BBC London**. [*s.l.*]; [*s.n.*], 30 maio 2023. 1 vídeo (5 min). Publicado pelo canal Nora Fakim. Disponível em: https://tinyurl.com/29jbdf3m. Acesso em: 19 nov. 2024.

BÜRGE, C. **How AI is fuelling fake vacation rentals in London | AirBnB rental roulette**. [Vídeo]. RTS Radio Television Suisse, 27 set. 2024. Disponível em: https://t.ly/zeooI. Acesso em: 18 nov. 2024.

CARVILLE, O. Airbnb is spending millions of dollars to make nightmares go away. **Bloomberg**, 15 jun. 2021. Disponível em: https://t.ly/OcvCU. Acesso em: 17 nov. 2024.

CHATTERJEE, D.; DANDONA, B.; MITRA, A.; GIRI, M. Airbnb in India: Comparison with hotels and factors affecting purchase intentions. **International Journal of Culture, Tourism and Hospitality Research**, v. 13, n. 4, p. 430–442, 2019. DOI: https://doi.org/10.1108/IJCTHR-12-2018-0180.

CHEN, H.; BEAUDOIN, C.; HONG, T. Securing Online Privacy: An Empirical Test on Internet Scam Victimization, Online Privacy Concerns, and Privacy Protection Behaviors. **Computers in Human Behavior**, v. 70, p. 291-302, 2017. DOI: https://doi.org/10.1016/j.chb.2017.01.003.

CHRISTIN, G. A. D.; NUGRAHA, A. K. N. The Impact of Online Review and Price on Consumer's Hotel Booking Intention at Online Travel Agency: Trust as a Mediating Variable. **International Journal of Electronic Commerce Studies**, v. 13, n. 4, p. 159, 5 jan. 2023.

CLARK, J.; WOOD, Z. **Victims speak out over 'tsunami' of fraud on Instagram, Facebook and WhatsApp**. 16 jun. 2023. Disponível em: https://shorturl.at/5so88. Acesso em: 18 nov. 2024.

CONTI, A. I accidentally uncovered a nationwide scam on Airbnb. **Vice**, 31 out. 2019. Disponível em: https://t.ly/9hvBD. Acesso em: 17 nov. 2024.

CROPLEY, D. H.; CROPLEY, A. J.; KAUFMAN, J. C.; RUNCO, M. A. **The Dark Side of Creativity. Cambridge**: Cambridge University Press, 2010. DOI: https://doi.org/10.1017/CBO9780511761225.

CUDD, G. **Fiverr scams**: What they are and how to avoid them. Don't Do It Yourself, 2022. Disponível em: https://t.ly/t6Pju. Acesso em: 18 nov. 2024.

DENT, S. Uber sued by more than 500 women over sexual assault and kidnapping claims. **Engadget**, [*s.l.*], 14 jul. 2022. Disponível em: https://t.ly/xjzna. Acesso em: 21 nov. 2024.

DING, X.; MURPHY, L.; CHEN, T.; PEARCE, P. L. Differentiating tourist scam cases: Towards a taxonomy of deceptive schemes. **Journal of Hospitality and Tourism Management**, v. 50, p. 159–167, 2022. DOI: https://doi.org/10.1016/j.jhtm.2022.01.011.

EKSTEIN, N. Airbnb is fundamentally broken, its CEO says. He plans to fix it. **Bloomberg**, 2 out. 2023. Disponível em: https://tinyurl.com/ydz2fm52. Acesso em: 18 nov. 2024.

ELIOT, L. Generative AI ChatGPT as masterful manipulator of humans, worrying AI ethics and AI law. **Forbes**, 1 mar. 2023. Disponível em: https://tinyurl.com/anpmxbwz. Acesso em: 18 nov. 2024.

FARMAKI, A.; KANIADAKIS, A. Power dynamics in peer-to-peer accommodation: Insights from Airbnb hosts. **International Journal of Hospitality Management**, v. 89, p. 102571, 2020. DOI: https://doi.org/10.1016/j.ijhm.2020.102571.

FERGUSSON, A. 127,183 Airbnb guest complaints expose scams, safety concerns, infestations and more. **Asher and Lyric**, 11 out. 2021. Disponível em: https://tinyurl.com/5usednsm. Acesso em: 19 nov. 2024.

FICHNOVÁ, K. **Psychology of creativity for marketing communication**. Selected aspects. Association Amitié Franco-Slovaque, 2013.

GALLAGHER, L. **The Airbnb story**. Mariner Books, 2018.

GEBBIA, J. **How Airbnb designs for trust**. [*s.l.*]; [*s.n.*], 2016, 1 vídeo (17 min). TED. Disponível em: https://tinyurl.com/y6td6wtx. Acesso em: 17 nov. 2024.

GERKEN, T. Booking.com warns of increase in travel scams. **BBC**, [*s.l.*], 21 jun. 2024. Disponível em: https://tinyurl.com/yc7pk66e. Acesso em: 22 nov. 2024.

GRAVES, L. Understanding the promise and limits of automated fact-checking. **Reuters Institute for the Study of Journalism**, 1 fev. 2018. Disponível em: https://tinyurl.com/ycky4upz. Acesso em: 22 nov. 2024.

HARTMANS, A. Airbnb now has more listings worldwide than the top five hotel brands combined. **Business Insider**, 10 ago. 2017. Disponível em: https://tinyurl.com/tu3yz7ew. Acesso em: 18 nov. 2024.

KAČINOVÁ, V. Press agencies as fact-checking tools in media education on disinformation: A case study of the TASR in comparison with the APA. **Medien in der Jugendarbeit/Median Impulse**, v. 1, p. 13, 2022. DOI: https://doi.org/10.21243/mi-01-22-13.

KAPOOR, H.; PUTHILLAM, A. The Crisis of Misinformation and Dark Creativity. Springer EBooks, p. 179–203, 2024. DOI: https://doi.org/10.1007/978-3-031-61782-9_9.

KEY, K. Travel warning: Look out for AI booking scams. **PC Magazine**, 31 ago. 2024. Disponível em: https://tinyurl.com/4zvtsjn7. Acesso em: 19 nov. 2024.

KIELY, T. J. **What is desk research**? Meaning, methodology, examples. Meltwater, 2024. Disponível em: https://tinyurl.com/27suzww8. Acesso em: 18 nov. 2024.

MAO, Z.; WEI, W. Sleeping in a stranger's home: a trust formation model for Airbnb. **Journal of Hospitality and Tourism Management**, v. 42, p. 67-76, 2019.

MARR, B. A short history of ChatGPT: How we got to where we are today. **Forbes**, 19 maio 2023. Disponível em: https://tinyurl.com/pd3s77k8. Acesso em: 18 nov. 2024.

MILLER, E. J.; STEWARD, B. A.; WITKOWER, Z.; SUTHERLAND, C. A. M.; KRUMHUBER, E. G.; DAWEL, A. AI hyperrealism: Why AI faces are perceived as more real than human ones. **Psychological Science**, v. 34, n. 12, p. 1–14, 2023. DOI: https://doi.org/10.1177/09567976231207095.

MORBEY, M. L. **From canvas to computer: Harold Cohen's artificial intelligence paradigm for art making**. 1992. Doctoral dissertation – The Ohio State University.

NEW AirBNB scam, even airBNB fell for it! How to protect yourself and prevent it in future bookings! [*s.l.*]; [*s.n.*], 8 ago. 2022. 1 vídeo (14 min). Publicado por: Financial Life. Disponível em: https://tinyurl.com/24kmyuzx. Acesso em: 20 nov. 2024.

NIGHTINGALE, S. J.; FARID, H. AI-synthesized faces are indistinguishable from real faces and more trustworthy. **Proceedings of the National Academy of Sciences (PNAS)**, v. 119, n. 8, p. 1–3, 2022. DOI: https://doi.org/10.1073/pnas.212048111.

OOI, K.-B.; TAN, G. W.-H.; AL-EMRAN, M. *et al.* The potential of generative artificial intelligence across disciplines: perspectives and future directions. **Journal of Computer Information Systems**, p. 1–32, 2023. DOI: https://doi.org/10.1080/08874417.2023.2261010.

PAPASAVVA, A.; JOHNSON, S.; LOWTHER, E. *et al.* Application of AI-based models for online fraud detection and analysis. **ArXiv**, 2024. DOI: https://doi.org/10.48550/arXiv.2409.19022.

PHUA, V. C. Perceiving Airbnb as sharing economy: the issue of trust in using Airbnb. **Current Issues in Tourism**, v. 22, n. 17, p. 2051-2055, 2018.

POPOV, C. Up to 900% surge in travel scams, warns Booking.com. **Bitdefender Hot for Security Blog**, 21 jun. 2024a. Disponível em: https://tinyurl.com/2p9zpfer. Acesso em: 17 nov. 2024.

POPOV, C. Most Common Airbnb Scams by Hosts and Guests (and How to Avoid Them). **Bitdefender Hot for Security Blog**, 28 ago. 2024b. Disponível em: https://tinyurl.com/2s3fvz29. Acesso em: 19 nov. 2024.

REID, J. Risks of generative artificial intelligence (GenAI) – assisted scams on online sharing-economy platforms. **The African Journal of Information and Communication**, v. 33, n. 1, p. 1–21, 2024. DOI: https://doi.org/10.23962/ajic.i33.18162.

ROOSE, K. Can A.I. be blamed for a teen's suicide? **The New York Times**, 23 out. 2024. Disponível em: https://shorturl.at/RrsFJ. Acesso em: 25 nov. 2024.

SHAH, P. Facebook Marketplace's dirty dozen: The 12 most common scams and how to avoid them. **Android Police**, 12 maio 2023. Disponível em: https://tinyurl.com/4vdrsees. Acesso em: 19 nov. 2024.

SLAGLE, J. R. **Artificial intelligence**: The heuristic programming approach. McGraw-Hill, 1971.

SOUČEK, J.; JIZBA, R. Telekopye hits new hunting ground: Hotel booking scams. **WeLiveSecurity**, 24 nov. 2024. Disponível em: https://tinyurl.com/bde2ny7b. Acesso em: 23 nov. 2024.

STONE, B. **The upstarts**: Uber, Airbnb, and the battle for the new Silicon Valley. Back Bay Books, 2018.

TUSSYADIAH, I. P. An exploratory study on drivers and deterrents of collaborative consumption in travel. **INFORMATION and Communication Technologies in Tourism**. Cham: Springer, p. 817-830, 2015.

WACH, K.; DUONG, C. D.; EJDYS, J.; KAZLAUSKAITĖ, R.; KORZYNSKI, P.; MAZUREK, G.; PALISZKIEWICZ, J.; ZIEMBA, E. The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. **Entrepreneurial Business and Economics Review**, v. 11, n. 2, p. 7–30, 2023. DOI: https://doi.org/10.15678/EBER.2023.110201.

WALSH, C.; SAXENA, D.; MUZELLEC, L. Airbnb: Managing trust and safety on a platform business. **The Irish Journal of Management**, v. 39, n. 2, p. 126–134, 2020. DOI: https://doi.org/10.2478/ijm-2020-0004.

WHY online trust and safety is top of mind for the travel and hospitality industry. [*s.l.*]; [*s.n.*], 28 ago. 2024. 1 vídeo (26 min). Publicado pelo canal: Booking.com partners. Disponível em: https://shorturl.at/fkqu2. Acesso em: 19 nov. 2024.

ZAMANI, E. D.; CHOUDRIE, J.; KATECHOS, G.; YIN, Y. Trust in the sharing economy: The Airbnb case. **Industrial Management and Data Systems**, v. 119, n. 9, p. 1947–1968, 2019. DOI: https://doi.org/10.1108/IMDS-04-2019-020.

Acknowledgment

APVV-23-0612 Creativity as a source of prophylaxis against media hoaxes/CREativity Against HOaXes/CREATHOX.