(Un)Secure Booking: Security Risks Within Facebook Groups Accommodation Reservations

Mihaela Franjić, Barbara Pavlakovič Farrell
University of Maribor, Faculty of Tourism, Brežice, Slovenia
mihaela.franjic1@um.si, barbara.pavlakovic@um.si

The tourism industry has significantly reshaped with the development of ICT and the Internet. In the contemporary digital world, most tourists utilise Smart Tourism Technologies services to search and book their travels, pay for services, and discover attractions at destinations. The level of security is a significant factor affecting the tourist experience since tourists employ technology to obtain information in all stages of their travel, especially in the first phases, and trust that it is reliable and truthful. Among the most known threats are fake profiles, identity theft, personal data theft, AI fraud, and others. Facebook, a pioneer in social media, hosts various groups related to promoting tourism (advertisements, tourist communities, reviews) or tourism offers (transportation, accommodation, guided tours, equipment sales). There are increasing cases of Facebook booking scams, where users are paying money for tourism services but ending up without paid service. Therefore, this paper focuses on the booking phase by analysing providers' actions within Facebook groups regarding popular tourist destinations such as Amsterdam, Milan, Prague, Istanbul, London, and Dublin. By analysing written and visual content and carefully reviewing group posts and requests, we identified signs of potential security risks that users should be aware of when searching for providers.

DOI
https://doi.org/10.18690/um.fov.2.2025.19

ISBN
978-961-286-963-2

Keywords:
digitalisation, Protection Motivation Theory, tourism, cybersecurity, peer-to-peer accommodation, Facebook, scams

University of Maribor Press

1 Introduction

The tourism sector has widely welcomed the new digital era. The use of websites, social media and smartphones is on the rise and pervasive. Tourism today heavily relies on digital platforms, with consumers increasingly inclined to use various applications and websites (Kapera, 2022). We can describe digitalisation as "the integration of digital technologies into everyday life" (Kuhn & Margellos, 2022, pp. 93). Smart Tourism Technologies (STT) are, therefore everyday life of tourists and their travel. Crucial elements of STT services are personalisation, accessibility, an abundance of information, and interactivity; nevertheless, we emphasise another important element, and that is security. The level of security is a significant factor affecting the tourist experience since tourists employ technology to obtain information in all stages of their travel and trust that it is reliable and truthful. Recent trends show that researchers of digital in tourism are focused on malware detection, data mining and support vector machine when working within the cyber community (Sharma et al., 2023). These trends support the statement that cybersecurity is of the utmost importance.

With the increasing reliance on social media for travel-related arrangements, addressing the concerns associated with booking accommodation is essential. Fraudulent listings on such platforms pose a significant risk to travellers, especially those unfamiliar with digital security practices. To examine this issue, our study investigates deceptive accommodation scams by engaging students in a practical experiment and conducting a content analysis of scam-related discussions.

As a notable example of a security vulnerability, we emphasize the risks of booking accommodation via social media, particularly within Facebook groups. The primary objective is to identify potential cybersecurity threats that users should be aware of when searching for accommodation providers, along with suspicious behaviours or indicators that could compromise profile security.

Following an extensive literature review, this work presents examples of counterfeit profiles and deceptive accommodation offers identified across major European cities, including Amsterdam, Milan, Prague, Istanbul, London, and Dublin. Through content analysis, we extracted key indicators of fraudulent listings that could serve as valuable references for future accommodation searches. Grounded in the

Protection Motivation Theory, these findings aim to enhance tourists' cybersecurity awareness and provide them with practical tools to assess the credibility of social media profiles, ultimately enabling safer and more reliable booking decisions.

2 Literature review

Cybersecurity (also called information technology security) is defined as a set of mechanisms for ensuring security for different types of information technology systems, processes, data and information, software, computers, virtual resources, electronic devices, physical infrastructures and people in order to reduce unauthorised access or usage (Villalón-Fonseca, 2022; Kovačić, Čičin-Šain, & Milojica, 2022). This includes online platforms, payment processing systems, customer databases, and communication channels. All of these are widely used by tourists, travel agencies, hotels, airlines, private tourism providers and others. Therefore, the tourism and hospitality sector is not immune to fraud and scams and is facing an extensive increase in cybercrime (Waller & Bartlett, 2022). Studies show that tourists and tourism providers have encountered cyber-attacks, side jacking, point-of-sale attacks, insecure transactions, personal data breaches, and phishing (Ghaderi, Beal & Houanti, 2024). If we focus on scams, "a scam is a form of fraud that is achieved through trickery that results in financial gain for the perpetrator and financial loss for the victim. Scams have proliferated on online sharing-economy platforms, with such scams typically relying on varying degrees of misrepresentation for their success." (Reid, 2024, pp. 3).

The consequences of listed malpractice can be substantial financial loss, damaged reputation, and broken trust (Ghaderi, Beal & Houanti, 2024). Besides, customers' and employees' personal information (personal identity and contacts) can be compromised (Chen & Fiscus, 2018). Other consequences may be the influence on mental illness symptoms, a feeling of humiliation and worsening of personal relationships (Parsons, Pantridge & Flaherty, 2021). These are the reasons why the tourism sector has to perform cybersecurity risk assessment. Within this process, they identify the critical assets they need to protect, determine the possibility of risk realisation, recognise possible attackers, their motivation and mode of operation, and evaluate the impact of the attack on the organisation (Chen & Fiscus, 2018; Paraskevas, 2020).

All tourism sectors are prone to cybercrime. Several experts have researched tourism providers and their practices with cybersecurity. Florido-Benítez (2024) and El-Maksoud (2024) examined travel agencies and recommended more education on cybersecurity for employees and taking procedures to secure tourism networks to achieve the digital trust of customers. Berezina et al. (2012) focused on the hotel sector and confirmed that guests' credit card information breaches result in lower satisfaction and no revisiting intentions.

In tourism, booking accommodation through online platforms and social media is not a new phenomenon; it is a part of the sharing economy (Pouri & Hilty, 2021) and has been noticed for several years. More specifically, we can refer to it as peer-to-peer (P2P) accommodation, which works through online networking platforms where people rent out available space (a whole property or just a part of it) for a short period of time (Farmaki & Christou, 2019). The market leader is Airbnb, also known is couch surfing and similar organised providers. However, some individuals rent their property through social media.

As known, Facebook is a pioneer in social media. On its sites, there are various groups related to promoting tourism (advertisements, marketing, tourist communities, reviews) or tourism offers (transportation, accommodation, guided tours, equipment sales). There are also different types of scams on Facebook. Joy and Leroux (2024) list 15 types: Defective or counterfeit gadgets and electronic items; Bait and switch; Fake payment receipts; Mouth-watering giveaways; Overpayment by a buyer; Moving conversations out of Facebook; Fake rental posting; Advance payment requests; Asking for confirmation codes; Asking for car deposits; Requesting unnecessary charges; Mailing items; Fake claims of lost packages; Counterfeit money; Clicking a link to fill out more information. Relevant to our study is bait and switch, when tourists rent attractive-looking accommodation, which is later switched with an inferior one. Also important is fake rental posting, which is when scammers post fake rental properties (they do not own them or are not authorized to post them). They request an advance payment as deposits or background check fees from tourists or other interested people for renting the place. However, if a tourist visits the property, it is not available or does not even exist (Joy & Leroux, 2024).

The presented cases can be referred to as "phishing," a technique used in attacks to steal money, identity, and sensitive data, such as bank account information and passwords (Aleroud & Zhou, 2018). Through Facebook booking scams, the goal is to trick the victim into believing they are communicating with a trusted organisation. There are also scams, where customers believe they are interacting with services such as banks, online stores, or platforms like Booking or Airbnb. Van Der Zee, Clayton & Anderson (2019) call them "rental scammers", which are described as individuals who engage in advance fee fraud by pretending to be landlords and attempting to deceive victims into paying a deposit for an apartment that is not actually available for rent. These individuals use fake ads and information to create the illusion of offering actual apartments, misleading victims in order to take their money upfront, often before the apartment can even be seen or verified.

As mentioned, there are other social networks and alternative online booking methods. Reid (2024) focused on Airbnb and discovered that the development of Generative artificial intelligence (GenAI) might increase the misconduct behaviour of scammers on sharing-economy platforms. Using GenAI, inauthentic content can be produced quickly and cheaply (for example, aliases, fake profile images, fake property images, and fake property descriptions).

The online environment is highly liable to cybersecurity threats. Taylor, McDougall, Ollis & Alford (2019) examined several websites and analysed the viewers' trust in the website content. The conclusion was that websites can be designed to encourage more or less perceived trust. Therefore, viewers should be aware of the threats and verify "too good to be true" deals. Trust in the host has become a crucial element of online commerce since customers have to feel safe and believe that the purchase will fulfil their expectations without any harm (Nisar et al., 2020).

This statement is supported by the Protection Motivation Theory (PMT). It is defined as a pre-eminent health behaviour theory that emphasises behaviours which protect one's health, reduce risks or increase benefits for a person's well-being (Balla & Hagger, 2024). The concept of health-protective behaviour is also used in other fields, for example, cybersecurity and tourism. Here, PMT helps tourists gain insight into the risks that arise from the digital world. Tourists can identify their vulnerable points by rational thinking about the possibility of harmful events and can prepare to react or respond in appropriate, recommended ways (Ghaderi, Beal & Houanti,

2024). This includes protective measures such as using secure payment methods, caution about sharing personal data online, and checking websites and social media for security indicators. Especially the latter is the focus of this research. Examining different fake Facebook profiles, we tried to identify key security indicators that signal a clear security threat while booking accommodation on social media.

3 Method

After conducting a literature review, empirical data was collected through a practical experiment. Later, a content analysis of written and visual material was conducted to analyse the data. The practical experiment was done with the help of tourism students from the University of Maribor, Slovenia. Within their class about safety and security in tourism, one of the topics was current travelling problems, especially connected with cybersecurity and social media. There, the students were introduced to common fraudulent tactics used in online accommodation scams. That provided them with foundational knowledge on identifying potential threats when searching for rentals on social media platforms, which was their study task. Students focused on "rental scammers" on Facebook.

3.1 Guided Student Task

The research focused on Facebook groups dedicated to renting apartments in different cities across Europe (Amsterdam, Milano, Prague, Istanbul, London, Vienna, Berlin and Dublin). Firstly, students connected with Facebook accommodation rental groups/individuals and created a post using combinations of words that indicate travellers searching for accommodation rentals. Therefore, they described that they needed an apartment for themselves and their friends; they wrote how long they would stay; and what their budget was. Next, students engaged with responses received, documenting their interactions, observations, and key indicators of fraudulent behaviour. Screenshots of conversations enabled further content analysis and interpretations.

To ensure ethical compliance, all students voluntarily participated in the task and, after completing the exercise, deleted their posts and profiles. The collected data included screenshots of conversations, personal reflections, and comparative

assessments of legitimate versus fraudulent listings. All data is stored with the researchers.

3.2 Content Analysis of Scam-Related Posts

The second phase of the study consisted of an in-depth content analysis of scams identified in open Facebook groups for accommodation search. To detect fraudulent activity, we searched for key terms such as "phishing," "scam," "fake," and "fraud" using a personal account. Materials were mostly URLs of discussions, screenshots, conversations and descriptions of how tourists have been scammed.

We focused on posts from Europe and countries that are popular for their seasonal tourism (Italy, Austria, Croatia, Greece and others). We also searched for the reviews of the tourists who had bad experiences and have been scammed already including discussions on Reddit and Facebook. Reviews from scammed tourists were analysed and helped us to identify recurring patterns, emerging scam tactics, and common characteristics of deceptive listings.

4 Results

Based on our content analysis and discussions, we developed two tables to summarize our findings: (1) key fraud indicators - the most common warning signs of fraudulent listings and (2) recommended best practices for avoiding scams - recommended actions to mitigate risks, which are explained in following chapters.

4.1 Scam indicators

To better understand how rental scammers attempt to deceive their victims, we analysed their posts, comments, and messages. Indicators through which we can conclude that it is a scam are described in Table 1.

Table 1: How to recognise a rental scam?

Indicator	Explanation	Example
Fake rental listing	Scammers often create listings for properties that do not exist or are not available for rent. They may use photos and descriptions stolen from legitimate rental websites or hotels.	- The accommodation location is in town, but in the pictures, there is a sea. - A listing for a beachfront villa uses photos copied from a luxury resort's website. - The provider sends different (not matching) pictures of the apartment (for example, different styles of one bathroom on more pictures). - The provider says that it is a one-room apartment, but they sent a picture of a studio without the rooms.
Unusually low prices	Tourist accommodations in popular destinations often come at a premium price. Listings with prices significantly lower than the market average are a red flag for scams. Also, there is something unusual if the rent price is significantly lower than the market value per night/person.	- A luxury apartment in a prime tourist area is listed at half the price of similar properties. - Offering a discount/one more night when tourist moves to a private chat with providers.
Pressure to pay quickly	Scammers create a sense of urgency to pressure travellers into making hasty decisions, often claiming that the property is in high demand.	- The provider says that someone cancelled the booking, so they want to give a lower price and mention other tourists are waiting. - The lower price stands only within the next hour.
Request to pay in advance	Legitimate hosts typically do not ask for full payment or large deposits before the guest has seen the property or signed a rental agreement. Scammers have typical patterns that you need to send them a deposit. They often promise to secure your booking and may provide bank account details that do not match the name of the supposed host or property owner. They frequently request payment through fast transfer services, as these methods allow them to receive funds quickly and make it difficult to trace or recover the money.	- After a few exchanged messages, the provider mentions that the guest would need to pay 200 € in advance.
Moving the conversation or payment to another platform	Scammers may try to move communication or transactions off the original platform to avoid detection and make it harder for victims to report them.	- Providers often comment on the post "dm me". - Providers start the chat with the victim on Messenger. - "Let's discuss the details and payment on WhatsApp or email instead of here".

Indicator	Explanation	Example
Non-verified sender	There are profiles which are untrustworthy. Often, there is a lack of personal details, friends, posts and engagement in general. Scammers often use fake or newly created profiles with no information or activity history. These profiles are designed to disappear after the scam is complete.	- A profile with no photos, no friends, and only one post advertising a rental. - The provider is blocked by Facebook, and tourists are notified that he/she was a scammer. FB advised to block them everywhere and not to provide any personal or banking information. - A provider with a profile picture of a little girl who was presenting herself as a middle-aged man. - The profile contains no information, only a profile picture.
Poor English proficiency and generic responses	Usually, the messages that scammers send are poor in grammar, unity, coherence, presentation, and vocabulary. Messages are usually riddled with errors, incomplete sentences, or overly generic responses. Also, it is hard for them to chat like native speakers, especially in some less-known languages. They may struggle to answer specific questions about the property. They strive for the conversation to keep on going.	- The provider does not carefully read tourists' posts since they ask for already communicated information. - The provider posted a generic response: "Hello dear, the apartment is very nice and available. Send payment now to book."
Inconsistent or mismatched details	Discrepancies between the listing description, information, their role, and location.	- Sending an address of the accommodation of another accommodation (for example a rental in Amsterdam that is promoted on other platforms). - The provider represents his/herself as a help in search (not an owner).
Fake exclusivity or Commitment	Claims that the property is in high demand or requires an immediate commitment to pressure the victim. They use a "limited edition" type of persuasion, which is popular when you want to rush someone to buy something and decide on it. People often don't want to miss the chance.	- Provider mentions that the tourist is not the only one and that other people are interested, so the tourist needs to decide very quickly.
Kindness or Sympathy	Scammers may use overly friendly or emotional language to gain trust.	- Almost every conversation starts with "dear". - The provider offers extensive help with the price and searching.

Scams can be detected from various factors of the provider profile. One of the main factors is the age of the profile (a profile with no history) and profile pictures. Other factors include profiles, which send links to numerous non-credible websites (usually scam sites). Also, when providers are asked for a personal ID document, they send a fake document and immediately delete the conversation. The next factor is money since fake providers often ask for a 200-300 € payment upfront.

4.2 Recommendations for verification

While some individuals may immediately recognise that the profile and post are fake, others may reach out and realise later that the listings and offers are fraudulent. Some users even share advice on how to verify the legitimacy of such offers. It is essential for tourists to ask for more information to avoid falling for phishing scams and fake content.

In accordance with the Protection Motivation Theory, developing a set of criteria is crucial for distinguishing between fake and legitimate profiles, posts, comments, and other related content. Guidelines for tourists are presented in Table 2. However, even if the criteria can be satisfied, it can still be a case of a rental scam because scammers are getting better with time and experience.

Table 2: Guidelines on how to behave and respond to suspected scams

Recommendation	Explanation
Verify the identity/profile	Carefully examine the landlord's or host's profile for authenticity. Look for signs of a genuine user, such as a history of activity, real photos, detailed information, and interactions with others. Be cautious of profiles that appear incomplete or newly created. A profile with generic stock photos and no friends or reviews is the first "red flag".
Ask for legal documentation	Request official documents to confirm the legitimacy of the rental. This includes a rental agreement, proof of ownership, or a government-issued ID. Legitimate hosts will provide these without hesitation. Tourists can ask for a copy of the property deed or a utility bill in the host's name or request a signed rental contract before making any payments.
Use trusted platforms	Book through reputable platforms that verify hosts and properties (for example Airbnb or Booking.com). They are not 100% safe, but they provide secure payment systems and customer support to resolve disputes. Avoid deals arranged solely through social media or messaging apps and avoid booking through unverified Facebook groups or Craigslist.

Recommendation	Explanation
Search for reviews of accommodation	Tourists can look for reviews from previous guests to confirm the legitimacy of the property and the host. Looking for reviews that mention specific details about the property or host can help to recognise whether it is generated or not. They should not forget to be cautious if there are no reviews or if they seem overly positive and generic.
Search for an address in Google Maps	Verify the property's location and existence using Google Maps or Street View. Scammers often list properties in prime locations that don't exist or use fake addresses. Even if the address exists on Maps, there can be many concerns, especially when the listing is in the city centre and when the address leads to other organisation property.
Never share Personal Information	Avoid sharing sensitive information like passport details, bank information, or social security numbers unless absolutely necessary and verified. Scammers can misuse this information for identity theft. They can use your ID, data and information to scam other people, which is a very complicated situation.
Watch for unusual behaviour, inconsistencies	Be cautious if the host avoids answering specific questions, provides inconsistent details, or behaves suspiciously. Scammers often struggle to maintain a consistent story. If something feels off or too good to be true, it probably is. Don't ignore red flags, even if the deal seems attractive.
Search for the same pictures	Use tools like Google Lens or similar to check if the property photos appear on other websites or listings. Scammers often reuse photos from other sources to create fake listings. Do the cross-check listings and search for the same property on multiple platforms to ensure consistency in detail, photos, and pricing. Scammers often create multiple listings with conflicting information.
Consult Local Authorities	Contact local tourism offices or housing authorities to verify the legitimacy of the property and the host. They can confirm if the property is registered or if there have been previous complaints.
Avoid paying in advance	Never pay the full amount or a large deposit before seeing the property or signing a contract. Scammers often disappear after receiving payment.
Ask for the quote and invoice	Request a formal quote or invoice and ensure you receive a receipt for any payments made. This provides proof of the transaction and can be used to resolve disputes. The host should provide a detailed invoice with their contact information.
Make a video call	Request a live video tour of the property or visit it in person before committing. Scammers often avoid showing the property or make excuses for why they can't. The host can also refuse to do a video call or show the property. They can say that accommodation is currently reserved or occupied.
Ask others for opinion	Like on Reddit, tourists can share the listing with friends, family, or online communities to get a second opinion. Others may spot red flags someone missed.
Avoid Wire Transfers	Avoid payment methods that are hard to trace, such as Western Union, cryptocurrencies, or direct bank transfers to unknown accounts. These methods offer little to no recourse if something goes wrong.

The guidelines can help travellers avoid rental scams when booking tourist accommodations online. Some key recommendations include verifying the host's identity, using trusted platforms, and avoiding untraceable payment methods. On the other hand, traditional reservation methods can offer a sense of safety and security. Visiting a local travel agency or directly calling a hotel reduces the risk of encountering fake listings or fraudulent hosts, as tourists are dealing with verified businesses or individuals.

5 Conclusion

As shown through the research, there is a need for caution when booking accommodation on social media platforms such as Facebook. While these platforms offer convenience, they also expose users to significant risks, particularly in the context of rental scams. Interestingly, these platforms sometimes have built-in systems to help detect fraudulent listings, and posts from other users who wish to alert others about scams. However, there are cases where users still become victims of fraudulent activities, demonstrating the need for enhanced awareness and vigilance.

Rental scams often involve fake listings, unusually low prices, and pressure tactics to exploit victims. Key red flags include mismatched details, requests for advance payments, generated messages and poor communication. To protect themselves, individuals should verify listings, avoid off-platform transactions, and remain cautious of overly friendly or urgent messages. Awareness of these indicators is crucial to avoiding financial losses and ensuring safe rental experiences.

The recommendations outlined in the paper serve as a practical guide for travellers to navigate the complexities of booking tourist accommodations in an era where scams are increasingly common. By verifying listings, using secure payment methods, and relying on trusted platforms, travellers can significantly reduce their risk of becoming victims of fraudulent schemes. However, it's equally important to recognise that not all listings are scams, and an overly cautious approach can sometimes lead to missed opportunities. The key is to remain vigilant, trust verified sources and seek external opinions when in doubt. Ultimately, a balanced approach will help travellers enjoy safe and hassle-free experiences while minimising the impact of scams on their trust in the booking process.

While this study covered only several scam cases from Facebook groups, further analysis of other platforms should be considered. There are also other aspects of online booking frauds. The role of Artificial Intelligence (AI) in facilitating scams has already been detected. With advanced AI tools, scammers can create more convincing fake profiles, advertisements, and even correspondence, making it even harder for users to detect fraudulent activities. Therefore, research on AI usage will certainly be the focus of future studies.

Based on the Protection Motivation Theory and this research, we can conclude that it is crucial for tourists to learn how to identify key indicators that signal untrustworthy profiles and listings. They should also be aware of how to protect their personal data to avoid falling victim to scams.

Acknowledgment

The authors would like to thank the students of the Faculty of the Tourism University of Maribor, who gathered the data on fake Facebook profiles and actively searched for security risk examples.

References

Aleroud, A., & Zhou, L. (2017). Phishing environments, techniques, and countermeasures: A survey. *Computers & Security, 68*, 160–196. https://doi.org/10.1016/j.cose.2017.04.006

Balla, J., & Hagger, M. S. (2024). Protection motivation theory and health behaviour: conceptual review, discussion of limitations, and recommendations for best practice and future research. *Health Psychology Review*, 1–27. doi:10.1080/17437199.2024.2413011

Berezina, K., Cobanoglu, C., Miller, B. L. & Kwansa, F. A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management, 24*(7), 991–1010. doi:10.1108/09596111211258883

Chen, H. S. & Fiscus J. (2018). A need for cybersecurity risk assessment in the hospitality industry. *Journal of Hospitality and Tourism Technology, 9*(2), 223-234. Doi:10.1108/JHTT-07-2017-0044.

El-Maksoud, R.M.A. (2024). Exploring the Role of Cybersecurity in Enhancing Digital Trust of Egyptian Travel Agencies. *JAAUTH, 26*(1), 185–204.

Farmaki, A. & Christou, P. (2019). Examining 'Space' in Peer-to-Peer Accommodation Settings. *e-Review of Tourism Research (eRTR), 16*(2/3), 33-42.

Florido-Benítez, L. (2024). The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities. *Smart Cities, 7,* 475–495. doi:10.3390/smartcities7010019

Ghaderi, Z., Beal, L. & Houanti, L'H. (2024). Cybersecurity threats in tourism and hospitality: perspectives from tourists engaging with sharing economy services. *Current Issues in Tourism,* 1-16. doi:10.1080/13683500.2024.2353327

Joy, A. & Leroux, F. (2024). Facebook Marketplace's dirty dozen: The 15 most common scams and how to avoid them. *Android Police.* https://www.androidpolice.com/avoid-facebook-marketplace-scams/#mailing-items

Kapera, A. (2022). Cybersecurity in travel based on the opinions of university students engaging in tourism. *Geography and Tourism, 2*(10), 7–15. https://doi.org/10.34767/GAT.2022.10.06

Kovačić, M., Čičin-Šain, M. & Milojica, V. (2022). Cyber security and tourism: bibliometric analysis. *Journal of Process Management and New Technologies, 10*(3-4), 75–92.

Kuhn, B. M. & Margellos, D. L. (2022). *Global Perspectives on Megatrends: The Future As Seen by Analysts and Researchers From Different World Regions*. Stuttgart: ibidem.

Nisar, T. M., Hajli, N., Prabhakar, G. & Dwivedi, Y. (2020). Sharing economy and the lodging websites. Antecedents and mediators of accommodation purchase intentions. *Information Technology & People, 33*(3), 873-896, doi:10.1108/ITP-06-2018-0297.

Paraskevas, A. (2020). Cybersecurity in Travel and Tourism: A Risk-based Approach, in Xiang, Z., Fuchs, M., Gretzel, U. and Höpken, W. (eds) *Handbook of e-Tourism*, Cham: Springer Nature Switzerland AG, doi:10.1007/978-3-030-05324-6.

Parsons, F. J., Pantridge, M. J. & Flaherty, G. T. (2021). Cybersecurity risks and recommendations for international travellers. *Journal of Travel Medicine*, 1–4.

Pouri, M. J & Hilty, L. M. (2021). The digital sharing economy: A confluence of technical and social sharing. *Environmental Innovation and Societal Transitions*, *38*, 127–139.

Reid, J. (2024). Risks of generative artificial intelligence (GenAI)-assisted scams on online sharing-economy platforms. *The African Journal of Information and Communication (AJIC), 33,* 1–21.

Sharma, D., Mittal, R., Sekhar, R., Shah, P. & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization, 10*, 1–32.

Taylor, J., McDougall, S., Ollis, G. & Alford, P. (2019). Assessing User Perceptions of Trust and Security in Manipulated Versions of Low Trust and High Trust Tourism Websites. *e-Review of Tourism Research (eRTR), 16*(2/3), 165–174.

Van Der Zee, S., Clayton, R., & Anderson, R. (2019). The gift of the gab: Are rental scammers skilled at the art of persuasion?. 1–32 https://doi.org/10.48550/arXiv.1911.08253

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security, 120,* 102805, doi:10.1016/j.cose.2022.102805.

Waller, l. & Bartlett, E. (2022). *Tourism Resilience.* Kingston: Ian Randle Publishers.

About the authors

Mihaela Franjić is a teaching assistant and a researcher at the Faculty of Tourism, University of Maribor in Brežice, Slovenia. Her research interests extend beyond Tourism to include artificial intelligence, informatics, statistics, digital transformation, user experience and protected areas. Additionally, she teaches more than twenty different courses, with a particular focus on social media and tourism security. Everything that affects tourists and their safety is a highly interesting and largely unexplored topic, especially when it comes to sharing personal data online and communicating with others.

Barbara Pavlakovič Farrell is an assistant professor and a researcher at the University of Maribor, Faculty of Tourism, Slovenia. Her work and research fields cover various aspects of tourism, destination management, sustainability, industrial tourism, communication, and safety & security in tourism. She graduated in communication studies, developed her public relations skills in several organisations as a PR practitioner and continued her career in academia. Her published works include scientific articles, books and book chapters about industrial tourism, HR, safety and security in tourism, sustainability and renewable sources, and conference contributions about the mentioned topics.