Risks of generative artificial intelligence (GenAI)-assisted scams on online sharing-economy platforms

Julie Reid
Professor, Department of Communication Science, University of South Africa (UNISA), Pretoria
https://orcid.org/0000-0002-7082-7834

Abstract
The prevalence of scams proliferating via online platforms has been identified as an emerging societal problem resulting in large-scale financial losses for victims. Online scams typically rely for their success on the generation of fake but convincing user profiles to conceal the identities of the scammers from the people being tricked into parting with their money. The increasing sophistication of generative artificial intelligence (GenAI), which can produce outputs indistinguishable from real content, thus carries the risk of being adopted by fraudsters to assist in the enactment of online scams. This article considers the risks of the potential uptake and use of GenAI applications by online scammers operating in the sharing economy, with a focus on homestay-marketplace platforms and, in particular, the largest such platform, Airbnb.

Keywords
online scams, fraud, artificial intelligence (AI), generative artificial intelligence (GenAI), sharing economy, homestay-marketplace platforms, Airbnb

DOI: https://doi.org/10.23962/ajic.i33.18162

Recommended citation
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. https://doi.org/10.23962/ajic.i33.18162

1. Introduction

Recent years have seen significant advancement in the sophistication, accessibility, and adoption of technologies rooted in artificial intelligence (AI) and machine learning. This growth trend is projected to continue in the immediate future. The extensive range of AI applications includes systems designed for the prevention and detection of criminal activity. Conversely, the technology also carries the risk of being misused to facilitate crime, with the potential for criminal exploitation increasing concomitantly with the expanding capabilities and adoption of AI tools. Some AI-facilitated threats emerge as an extension of pre-existing criminal activity, whilst others are novel, and such threats can, for the most part, be generated by using AI tools that are openly available to the public.

Recent explorative research efforts have sought to identify and pre-emptively anticipate potential threats from AI-assisted crime (Caldwell et al., 2020; Cross, 2022; King et al., 2020; Wach et al., 2023). Such studies have tended to focus broadly on crime in general and on AI in general, without a specific focus on the crime and AI sub-sets. The focus of this article is on the crime sub-set of online scams and, in relation to online scams, the specific threats posed by generative AI (GenAI). In many cases, online scams are enabled by the digital distribution of a message that involves some form of trickery or misrepresentation, where scammers falsely advertise services or products, or impersonate someone they are not, with the goal of financially or personally exploiting victims (Brooks, 2023). Given the increasing sophistication of GenAI, and the fact that its outputs are becoming impossible for human users to detect as not real (Miller et al., 2023; Nightingale & Farid, 2022), I discuss the implications thereof, and whether this technology could lead to an expansion of online scam operations.

Whether operating as social media sites, sharing-economy platforms, or e-commerce marketplaces, the central premise of several big tech online platforms is that they allow users to connect with one another online for the purpose of value exchange, with that exchange being either social or commercial. In many cases, these digital platforms have become ubiquitous and central to contemporary life, generating global user bases measured in billions. The prevalence of online scams that proliferate via popular big tech platforms has been identified as an emerging societal problem and has drawn the attention of lawmakers. For example, in the UK, Members of Parliament have argued that online platforms ought to be required to protect their users from fraudulent advertisements and scams (Thomas, 2022), and bankers have called on social media companies to reimburse victims of online fraud, accusing them of profiting from the scams proliferating on their platforms (Clark, 2023).

Social media users have been lured into scams via platforms such as Facebook, Instagram, and WhatsApp (Clark & Wood, 2023), often incurring considerable financial losses while enduring emotional anguish. Equally, users of sharing-economy and e-commerce websites have also been lured into scams through the false representation of various services or products, as is discussed in more detail below.

In this article, I consider the potential uptake of GenAI applications by scammers for use in acts of deceptive speech online on homestay-marketplace platforms, with a specific focus on Airbnb.

2. Objectives, definitions, and methodology

A great deal of existing literature and public debate is focused on the ethical and social ramifications of AI, and on regulating and controlling its civil uses, including, for example, in the education sector (Zawacki-Richter et al., 2019) and digital content creation (Hermann, 2021). AI-assisted crime, as a distinct phenomenon, has yet to be broadly recognised as an important area for study (King et al., 2020). Nonetheless, a limited collection of recent research studies has considered the potential of AI to assist bad actors in committing crimes (see Caldwell et al., 2020; Cross, 2022; King et al., 2020). Since the widespread adoption of AI tools available for public use is still a recent development, the field of studies of AI-assisted crime is symmetrically young. Understandably, the problem has several facets and possible use-case scenarios for the adoption of AI in crime that have yet to be investigated or critiqued by literature. This article aims to contribute to filling this research gap, to a limited degree, by foregrounding the possible uptake of GenAI by online scammers in the realm of one type of online sharing-economy platform: homestay marketplaces.

Definitions of AI are contested (García-Peñalvo & Vázquez-Ingelmo, 2023), and the term is applied in many contexts that do not result in the production of content. In this article, I concentrate specifically on GenAI—or, more specifically, on openly available machine-learning technologies that produce content (text, images, audio, or video) directed by prompts or inputs of the user via a front-end user interface.

Crime includes a broad range of criminal acts, including 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.

The purpose of this study was to explore the extent to which GenAI holds the potential to be adopted as a new tool by scammers to assist their activities. The contribution made by this study can only be classified as speculative, as there is, at present, no empirical evidence available to measure the adoption and use of GenAI by scammers in acts of deceptive speech online. Measurements of the adoption of

GenAI by online scammers might be provided in future reports by monitoring or law enforcement agencies that collect victim reports, but these are yet to be compiled or published. Also, while technologies for the detection of GenAI content are under development and could possibly be of use in research in future, these are currently lagging in developmental progress relative to GenAI applications (Heikkilä, 2023). Currently, research efforts aiming to perform direct measurements of scammer-produced online content would be hampered in the identification of such content for inclusion in a data corpus since AI-generated material is often indistinguishable from genuine content (Miller et al., 2023; Nightingale & Farid, 2022).

Accurate measures of the quantity and frequency of online scams are also difficult to establish since the domain in question is extremely broad, presumably present on the platforms of all large online-intermediary platform firms. For example, scams involving deceptive communications proliferate via email (Isacenkova et al., 2014) and text messaging (McCormick, 2023) campaigns, and on Facebook (Shah, 2023), Instagram (Clark & Wood, 2023; Stouffer, 2022), YouTube (Patel, 2023), Uber (Dent, 2022), Lyft (Holmes, 2019; Kerr, 2019; Turkos, 2019), Airbnb (Fergusson, 2021), Crewbay (Gillespie, 2023), Tinder (Ropek, 2022), Grindr (Igual, 2018; Igual, 2023; Sekudu, 2023), Amazon (Jones, 2023; Walsh, H., 2023; Wood, 2023), Trustpilot (Marsh, 2023), Tripadvisor (Giuffrida, 2018; O'Neill, 2018; Tripadvisor, 2023), Booking.com (Low & Fakim, 2023; Mann, 2019; Vahl, 2022) and several others. The enforcement and crime prevention authorities of various countries release periodic reports detailing indicators such as fraud reportage statistics and gross losses (ABS, 2023; Brooks, 2023; Mzekandaba, 2023; UK Finance, 2022). Such reports, while conducted sporadically, depending on the resources and research capacity employed by each country's investigative agencies, and while unable to provide a combined global measurement, nonetheless indicate that the proliferation of online fraud and scams is enormous.

The insights offered in this article are informed by the examination of a dataset that I collected for a separate research project, which investigated the structure of mediated communicative practices used by scammers to lure victims via Airbnb.[1] The methodology comprised a netnographic thematic qualitative content analysis of 600 units of user-generated content in which victims related their personal experience of being scammed via Airbnb. Units of analysis were sourced from the public submissions blog Airbnbhell.com, the open-access archive of the Better Business Bureau, TikTok,

1 The earlier study mentioned here culminated in a book manuscript, entitled *Delusive Speech in the Sharing Economy: Scam Inc.* (Taylor and Francis, New York), the publication of which is forthcoming at the time of writing.

and YouTube. Selected findings emanating from this dataset are discussed narratively below. Desktop research for the earlier study focused on contextualising Airbnb within the broader sharing economy and e-commerce spheres, and included scrutiny of news media reports of scam proliferation on other platforms such as Booking.com, Uber, Grindr, and Facebook Marketplace. The findings of the earlier study did not extend to exploring the potential adoption of GenAI by scammers in their deceptions.

3. Literature review and contextualisation of the problem

Much of the public discourse on GenAI has, to date, been centred 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 human-like 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., 2023; Ooi et al., 2023).

Through the testing of ChatGPT, Alawida et al. (2023) demonstrated how the chatbot can be manipulated by adversarial users in its response to cybersecurity questions to potentially orchestrate attacks by assisting in the development of polymorphic malware that can continually evolve, thus evading antivirus software. Other studies have explored the possibilities of ChatGPT being used "by adversaries to create social engineering attacks, phishing attacks, automated hacking, attack payload generation, malware creation, and polymorphic malware" (Gupta et al., 2023), and to generate harmful, inappropriate, offensive, or incorrect text and information (Liu et al., 2023). 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's behaviour, perceptions, and emotions (Wach et al., 2023).

In addition to textual outputs, GenAI technologies also provide the capabilities for the production of video, audio, and pictorial outputs that may be used by bad actors for nefarious purposes. Voice-cloning software can be used, for example, to extract funds from victims when a scammer uses the application to clone the voice of a loved one claiming to be in trouble. Such was the case with a father in the US city of Philadelphia who became the victim of a voice-cloning attack when he believed that he heard the voice of his adult son, who said that he had been arrested and urgently required USD9,000 for a lawyer (Rushing, 2020). Helmus's (2022) assessment of the risks posed by GenAI emphasises how deepfake content could be used to manipulate elections through the distribution of disinformation, to exacerbate social divisions, and to undermine sources of legitimate information, including professional

journalism. Deepfake video content could conceivably sway election outcomes if, for example, at the time of closely contested elections, deepfake videos are generated that portray candidates engaged in illicit or nefarious activities to damage their reputations (Helmus, 2022).

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. Cross (2022) investigates how GenAI images can be used in the facilitation of romance scams. Such scams are a fast-growing fraud category (Cross, 2023). In the US, the Federal Trade Commission (FTC) reported over 56,000 victims suffering losses of over USD547 million in romance fraud in 2021, an 80% increase on reported losses for the previous year (FTC, 2022). In the United Kingdom, romance fraud increased by 73% in 2021 relative to 2020, with GBP30.9 million lost (Clark, 2022).

Referred to by a variety of names including romance-baiting, pig-butchering, or cryptorom, online romance scams involve a high level of communicative deception on the part of the scammer, who typically employs a fake identity and alias. The victim is lured into what appears to be a genuine relationship via an online platform with the scammer who poses as a romantic interest. After rapport and trust are established, the scammer lures the victim into performing money transfers or depositing investments into fake cryptocurrency exchanges (Cross, 2023). Once the victim realises that they have been scammed, the effect can be devastating due to what has been termed the "double hit" of victimisation (Whitty & Buchanan, 2012). Not only does the victim lose money, but they must also grieve for the loss of what they believed to be a genuine relationship.

Prevention messaging and advice promoted by law enforcement and fraud monitoring agencies typically encourages users to protect themselves by verifying the identity of their online love interest by performing a reverse image search of profile pictures and images using tools such as Google Images or TinEye (Cross, 2022). Such actions may reveal whether an image has been plagiarised from an authentic source in an act of identity theft for the purpose of creating a fake profile. However, many deepfake images, and wholly synthesised images, cannot be tracked by such reverse-search tools, with the result that such tools have the potential to create the mistaken

impression that an image is genuine, thus increasing the vulnerability of a potential romance scam victim (Cross, 2022).

In addition to romance scams, there are several other online domains where the successful perpetuation of scams relies on acts of deception that rest on the generation of fake profiles and identities. The COVID-19 pandemic and lockdowns generated an explosion of internet pet scams, especially prevalent in Australia (May, 2022). Long-term lockdowns in some areas, a shortage of real animals, and the psychological need for company amid the isolation of extended lockdowns created a climate ripe for pet scammers online. The lockdown restrictions made it difficult for purchasers to see pets in-real-life before buying them, so acquiring them online seemed like a logical option. Scammers using fake identities and aliases took payments for animals that did not exist, via online marketplaces, classified ad websites, and even professional-looking websites that scammers set up to pose as legitimate breeders (through plagiarising the pet images, testimonials, or content of legitimate pet selling sites). Pet scams reported to the Australian consumer body surged by almost 1,000% in 2020, and gross losses exceeded AUD4.2 million in 2021 (ACCC, 2022; Kennedy, 2022).

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, but without delivering the services paid for (Cudd, 2022). Facebook Marketplace allows sellers and buyers of consumer items to connect with one another directly, minus a "middleman". Scammers on the platform use various tactics of deception, which include the advertising of counterfeit, defective, or entirely fictious items; fake giveaways constructed to steal confidential personal information; and forged payment receipts displaying a supposedly successful payment for an item (Shah, 2023).

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). The degree of sophistication and ease of use of such technologies offer a potential boon for online scammers across the entirety of the digital realm.

4. Scams on Airbnb that could be assisted by GenAI

An online homestay-marketplace platform, Airbnb's business model is two-sided, matching guests/travellers with hosts (property owners). Airbnb facilitates potential value creation on both sides of the exchange. Guests can gain access to cheaper accommodations relative to hotels, while hosts can earn income from otherwise underused space. Founded in 2007 and with more than 8 million property listings on its platform as of June 2024, Airbnb is the largest online homestay-marketplace platform, and provides more rooms worldwide than the top five hotel chains combined (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, C. et al., 2020). Airbnb is populated entirely with user-generated content. Property listings are produced by host users, reviews are authored by host users and guest users, and the platform provides a private messaging service similar to those found on social media apps such as Instagram or Facebook.

Several types of scams proliferate on Airbnb, all of which involve deceptive communication at the first point of contact on the platform between the guest user and the host user (the homestay rental advertiser). In going through the primary data collected—the aforementioned 600 units of user-generated content in which victims discussed being scammed via Airbnb—I identified three scam modalities in which scammers' fraudulent behaviours could potentially be assisted by the use of GenAI:

- bait-and-switch scams;
- fake-listing scams; and
- fake host-review scams.

Bait-and-switch scams

Bait-and-switch is widely recognised as a fraudulent activity whereby a company or business advertises a product well below its market price with the aim of substituting it with inferior or more expensive alternatives at the time of purchase (CFI, 2023). This type of fraud has been reconfigured by scammers on homestay-marketplace platforms. A scammer "host" will publish an attractive-looking accommodation listing at a price lower than competitors in the same region. The listing often does not represent a real property and is fake. The fake property listing is, in this case, the "bait".

Prior to the introduction of openly available GenAI technologies, such property listings were predominantly constructed as a collection of user/scammer-generated content, which involved the authorship of fictional property descriptions, plagiarising property images from elsewhere on the internet (often from real estate agent websites),

and plagiarising images of real persons (often from social media) for use as a fake profile image (along with an alias) to conceal the scammer's identity. The production of an inauthentic property listing would therefore require scammers to manually source or plagiarise relevant material. However, with the introduction of free-to-use GenAI applications, all such fake content can be produced much more quickly and easily, and at much greater scale. Importantly, prior to GenAI, users could use reverse-search applications to test the progeny of property images or host profile images, thus exposing a property listing as fake. But, as discussed above, wholly synthesised images cannot be traced by reverse-search tools, meaning that reverse-search tools may falsely identify an image as authentic (Cross, 2022).

On viewing the inauthentic listing, a guest user will reserve the property and pay for the booking. Close to the arrival time of the guest, and often just before or just after check-in time, the guest will receive a message from the "host", explaining that the property is suddenly unavailable due to an unforeseen emergency, such as a blockage in the plumbing. The scam host then explains to the guest that an alternative property is available and asks the guest to relocate to the alternative property. In this moment, the scammer now relies on the guest's natural feelings of panic and desperation.

Fearing being stranded without a place to stay, the guest is often left with little option but to accept the offer of an alternative property. This second property, comprising the "switch", is often sub-par, e.g., unsanitary, unsafe, and/or lacking in the amenities included in the original fake listing. Therefore, the guest pays for a premium property but stays in a rental that is not worth the amount paid.

Airbnb allows hosts to choose the cancellation policy for their listing from several alternatives. The "flexible" cancellation policy option allows guests to cancel up to 24 hours before check-in and receive a full refund, while the "strict" cancellation option requires guests to cancel within 48 hours of booking and at least 14 days before check-in. Under the "strict" option, hosts will be reimbursed 50% for all nights if guests cancel between seven and 14 days before check-in. The host will receive 100% of the lodging booking charge for all nights if the guest cancels after that. (There are also "moderate" and "firm" options of less severity than the "strict" option, but less flexible than the "flexible" option.) (Airbnb, n.d.-a). Airbnb's intention is to protect honest and genuine hosts from frivolous and unreliable guests, but scammers use the strict option to their advantage. The scammer waits until check-in time before switching the guest to the sub-par property, so that under the strict cancellation policy it is already too late for the guest to cancel the booking, and the host receives 100% of the booking fee. The guest is left with little recourse and no rights of redress since, according to the Airbnb system, the guest has "checked in" and the stay has proceeded as planned (Fergusson, 2021).

One Airbnb user—whose written account is included in the aforementioned 600-item dataset that I collected—described her bait-and-switch experience in Paris as follows:

> I received an email that my Airbnb flat wasn't accessible 10 minutes before arriving on site. I was offered a different flat in exchange which was 7 km from the original one. I took it and spent the night there.

The following morning this same user was again switched to another alternative location by the host, of which the user wrote:

> When entering the location, I found a tiny room without daylight, dirty cupboards as if just installed, and so small that opening the only sofa for sleeping meant not having space left to move anymore. I felt very uneasy because of this unprofessional treatment. When I saw the dirt on the cupboard I had had enough and booked a hotel nearby.

Another Airbnb user booked a penthouse apartment in the US city of San Diego two months ahead of a planned trip. The online listing for the property indicated that it had several luxurious amenities, including a swimming pool and outstanding views. In recounting what happened, the user wrote the following:

> About an hour before checking in, the host cancelled, and I was offered another Airbnb. It did not have a view like the penthouse did. I went to the address [of the alternative property] the host provided to find out they had a very strict policy against Airbnb in the building. They only lease to corporate clients and when I showed them the pictures they confirmed it was their building. They were pissed. I had been baited with the pictures and the view. They tried to switch me to another lesser property claiming maintenance issues. These bait and switch artists should be arrested for fraud.

The bait-and-switch scam finds nuance in the multiple-listings scam, where the advertised property is real but is listed multiple times. Bait-and-switchers list the same property with slightly different descriptions but at drastically different prices, thus charging varying prices for the same property. These multiple listings can all be placed on Airbnb or can be placed on several homestay-platform platforms, e.g., Airbnb, Booking.com, Hotels.com, or VRBO. If one guest books the property at a cheaper price and a second person books it at a higher price, the scam host will cancel the initial guest's booking. But the host will wait until the original guest arrives to check in before informing them of the cancellation, at which point the host will attempt to switch the first guest to the alternative sub-par property that is not equal in value to the property originally booked.

Fake-listing scams

In this second scam category, the property offered via the platform is entirely fictional. The published listing is constructed using the same tactics of deception as used for bait-and-switch, but is not connected to an alternative actual property. As with bait-and-switch, the scam "host" uses an alias together with a fake profile picture. The guest reserves and pays for the booking, but when arriving for check-in at the address listed on the booking confirmation, they discover that the property does not exist.

The scammer again makes use of Airbnb's "strict" cancellation policy (as explained above) and will not notify the guest that anything is amiss, waiting until the check-in time to be assured of earning the full booking fee despite the non-existence of the property advertised. While the guest may apply to Airbnb for a refund, these refunds are subject to a case review by Airbnb, which includes contacting (or attempting to contact) the "host", all of which takes time. Even if a refund is approved, this can take up to 15 days to clear in the guest's bank account (Airbnb, n.d.-b), which is of little use to the guest needing to make a same-day booking to replace the cancelled Airbnb. Because same-day reservations are more expensive than booking in advance, the reimbursement is unlikely to cover the inflated cost of the new booking, meaning that even a refunded guest suffers financially.

In the words of an Airbnb user travelling to Dublin:

> I found a great apartment listed normally along with lots of others on Airbnb. This listing turned out to be completely fake.

Another Airbnb user had a similar experience upon arriving in New York:

> We caught a cab and gave the driver the address of the Airbnb we booked. He pulled up to a parking lot and said, "this is it". We got out and went up and down the street trying to find the address. It was non-existent; there was no such address. It was rush-hour, 85+ degrees and we had gotten up at 4:00 AM. Needless to say, we were frantic. Then we had to find a hotel, which, obviously, was a lot more expensive.

Also in New York, a similar scenario unfolded for an Airbnb user who thought he had booked an apartment near Central Park:

> The host contacted me with information on how to receive the keys, and asked about my stay and how he could help with suggestions. After arriving at the "place" we found that the building had been torn down (the police said three years ago …), I was effectively stranded with nowhere to go; we had to book the only hotel we could find available for $500.

In Boston, an Airbnb user found himself directed to an office building by a scam host:

> I had made a reservation through Airbnb for a one-night stay at a studio apartment. I reached the address at around 6:00 PM. To my surprise, the building at the address was an office and there were no apartments. A situation had arisen where I had to spend the night on the side of the road or the lobby of this office building. I had to make last minute arrangements for an alternative stay. The last-minute arrangements cost me an additional $215. Airbnb and its hosts can leave you stranded in a foreign land without shelter, and as a result spoil your holiday by gifting you the worst mental agony.

Fake listings scams have long proliferated on Airbnb and have received a notable amount of news media attention (Conti, 2019; Temperton, 2020). In September 2023, Airbnb announced that it had successfully removed 59,000 fake listings and prevented another 157,000 from joining the platform in the 2023 year (CBS News, 2023).

Fake host-review scams

Airbnb employs a two-way reputation system of review; after the conclusion of their stay, guests review the property and the hosts, and the hosts similarly review the guests. This scenario is meant to prompt guests to respect the property of hosts, knowing that negative reviews of their behaviour could result in future booking request rejections. Equally, the system is designed to prompt hosts to deliver a satisfactory experience for guests, where multiple good reviews can result in a future increase in guest bookings and increased earnings. Investigative media reports (Conti, 2019; Temperton, 2020) and research studies (Bélanger De Blois, 2021) have tracked how scammers create fake host review networks on the platform to inflate the reviews and ratings of scam property listings with inauthentic positive feedback. This act of deception can be used to make bait-and-switch properties or fake listings appear more attractive to future unsuspecting guests.

Fake host-review networks can be engineered by a single individual or a collection of scammers working in collaboration. Scam hosts create a network of multiple fake host accounts, each connected to scam property listings. The scam hosts also open multiple fake guest accounts, and reserve stays at the properties advertised by the same scammer's fake host accounts. A fake "guest" then pays the fake "host" for a stay (both the guest and the host are the same scammer, or are scammers in cooperation), and the reservation proceeds via the platform as if a stay has actually taken place. The fake guest then publishes a positive review of the fake host and the fake host's scam listing.

The repetition of this process results in multiple positive guest reviews for scam hosts and scam listings—or, less damaging but still a scam, multiple positive reviews for actual properties that are of poor quality. As with bait-and-switch and fake-listing scams, fake host-review scams rely on the creation of multiple fake user profiles, aliases, and fake profile pictures.

Fake host-review scam networks routinely re-use the same property images, which have often been plagiarised from real property listings, across multiple fake listings in different locations and cities (Bélanger De Blois, 2021; Conti, 2019). Some Airbnb users picked up on this phenomenon.

One Airbnb user wrote that he

> […] took one of the photos of the scam apartment and scanned it through Google images; this apartment also appeared on another site with a different owner and another location.

In the words of another user:

> I found it sketcy [sic] and did research. I found out that they stole the listing information and pictures from [a competitor accommodation booking platform] and created a fake listing on Airbnb.

In another instance, an Airbnb host became aware that the images from his genuine listing had been plagiarised, and wrote as follows:

> I am a property owner in Mallorca, and it has come to my attention about two months ago that my photos have been duplicated and are being used by another host on a scam listing. I do not know this host and I have not given him permission to list my property anywhere.

5. Potential role and implications of GenAI-assisted online scams

As seen in the examples above from Airbnb, the guise of a fake profile becomes the enabler for multiple types of deception. While such scams have existed for some time and clearly pre-date the arrival of GenAI, the availability and use of increasingly sophisticated GenAI tools hold the potential to result in an acceleration of such scams online. For example, where a fake host-review network comprising 50 fake guest accounts would have previously taken a scammer days or even weeks of dedicated work to construct, the use of GenAI could reduce this production time to a few hours, meaning that the size of such networks could expand considerably.

Much of the architecture of the sharing economy relies on the user's faith in the notion of reciprocal trust. 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. For example, when hailing a car on a ride-sharing app like Uber or Lyft, the user must *trust* that the driver is a responsible vehicle operator. 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; Holmes, 2019; Kerr, 2019). 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.

Realising that trust and safety are central to the sustainability and profitability of its business (Airbnb, 2022; Gebbia, 2016; Zamani et al., 2019), Airbnb has established several multilayer defence mechanisms against scams (Airbnb, 2022; Ekstein, 2023; Gallagher, 2018; Jain, 2017; Walsh, C. 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 in spite of them scams still occur on Airbnb (Conti, 2019; Fergusson, 2021; Temperton, 2020) as scammers continually adapt to defences and seek out new ways to fool the system (Ekstein, 2023).

Helmus' (2022) assessment of the risks posed by GenAI includes the argument that the technology could erode trust in institutions and authorities, if the body of deepfake content in circulation represents persons of authority committing abhorrent acts. Equally, misinformation content, which could easily be generated with the assistance of GenAI, has been linked to lower levels of trust in the legitimate news media (Ognyanova et al., 2020). Business leaders have begun to express the sentiment that GenAI could erode customer trust in the commercial sector (Hill, 2023). Some AI watchers, including AI industry leaders, have claimed that the technology poses an existential threat, has the potential to result in human extinction, and ought to be prioritised for attention alongside societal-scale risks such as pandemics and nuclear war (Roose, 2023).

While I can offer no insights on the veracity of that somewhat alarming position, I do propose that GenAI-assisted scams could conceivably pose something of an

existential threat to sharing-economy platforms. If the technology is broadly adopted by criminals to assist in the enactment of scams on digital sharing-economy platforms, and if the frequency and volume of scams accelerate as a result, a broad dissolution of consumer trust is likely.

6. Conclusions

Originally defined at a Dartmouth College workshop in 1956 (Dartmouth, n.d.), AI has gone through various phases of theorisation and development, often in spurts of advancement, followed by periods of relatively slow progress sometimes referred to as "AI winters" (Sartori & Theodorou, 2022). The most recent AI summer, beginning roughly in November 2022 with the introduction of ChatGPT, has brought GenAI into focus and elicited much public debate. Throughout 2023 and 2024, discussions ranged from the topics of whether GenAI will displace workers due to automations causing disruptions in the workforce (Ooi et al., 2023) to whether the technology could be used to impact election outcomes (Helmus, 2022). I contend that the use of GenAI has further implications beyond those that have been most prominently contested in the public domain. In this article, I have argued that the development of GenAI, as evident in the emergence of applications for the generation of deepfake images and human-like text, has the potential to increase the ability of scammers to perpetuate crimes on various online platforms, particularly on sharing-economy platforms, owing to their reliance on user trust.

As mentioned in the Introduction, certain GenAI-facilitated risks arise as a continuation of pre-existing criminal activities—which can be amplified by GenAI tools that are readily accessible to the public. The three scam categories that I have assessed here are not novel and have proliferated on Airbnb for some time. Each of the three scam categories relies on the publication of inauthentic content including aliases, fake profile images, fake property images, and fake property descriptions. Prior to the introduction of free-to-use GenAI technologies, all such inauthentic content would need to be manually produced, or sourced (plagiarised), by scammers. Now, fake content can be produced much more quickly and easily, and in larger volumes, by leveraging GenAI, resulting in a risk that scammers will adopt GenAI to significantly expand their scam operations.

Currently there is no measurement of the rate of adoption of GenAI applications by scammers who operate on sharing-economy platforms. But given that GenAI can facilitate the rapid generation of convincing false user profiles, it is reasonable to assume that online sharing-economy scammers will adopt these applications. In the short term, this could conceivably place larger numbers of online users at risk of falling victim to scams. In the longer term, a resultant wide-scale dissolution of trust in sharing-economy platforms could undermine the business model of the online-intermediary platform firms that are currently some of the most valuable firms in the global economy.

It is crucial that further research considers GenAI's numerous potential social, cultural, and economic implications in increasing detail in order to, among other things, anticipate, and mitigate where necessary, possible future outcomes. Equally, it is incumbent upon GenAI product developers to acknowledge and assume responsibility for the potential ramifications of their work (Caldwell et al., 2020).

Funding
No funding was received for this study.

Data availability
The data supporting the results of this study is available upon written request to the author at reidjbj@unisa.ac.za

AI declaration
AI was not used in the writing of this article.

Competing interests
The author has no competing interests to declare.

References

Airbnb. (2022, May 13). *Airbnb launches the Trust & Safety Advisory Coalition*. Airbnb Newsroom.https://news.airbnb.com/airbnb-launches-trust-safety-advisory-coalition/

Airbnb. (2024, August 1). *Airbnb fast facts*. Airbnb Newsroom. Retrieved August 1, 2024, from https://news.airbnb.com/about-us/

Airbnb. (n.d.-a). *Cancellation policies for your listing*. Airbnb Help Centre. https://www.airbnb.co.za/help/article/475

Airbnb. (n.d.-b). *When you'll get your refund*. Airbnb Help Centre. https://www.airbnb.co.za/help/article/1967

Alawida, M., Shawar, B. A., Abiodun, O. I., Mehmood, A., Omolara, A. E., & Al Hwaitat, A. K. (2024). Unveiling the dark side of ChatGPT: Exploring cyberattacks and enhancing user awareness. *Information*, *15*(1), 1–26. https://doi.org/10.3390/info15010027

Australian Bureau of Statistics (ABS). (2023, February 22). *13.2 million Australians exposed to scams*. [Media release]. https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams

Australian Competition & Consumer Commission (ACCC). (2022). *Targeting scams. Report of the ACCC on scams activity 2021*. https://www.accc.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf

Bélanger De Blois, M. (2021). *Deceptive short-term rental operations*. [Master's thesis, McGill University, Montreal]. https://escholarship.mcgill.ca/concern/papers/08612t424

Bensinger, G. (2019, September 26). When rides go wrong: How Uber's investigations unit works to limit the company's liability. *The Washington Post*. https://www.washingtonpost.com/technology/2019/09/25/ubers-investigations-unit-finds-what-went-wrong-rides-its-never-companys-fault/

Brooks, K. J. (2023, October 6). Americans reported $2.7 billion in losses from scams on social media, FTC says. *CBS News*. https://www.cbsnews.com/news/online-fraud-losses-detection-social-media/

Caldwell, M., Andrews, J. T. A., Tanay, T., & Griffin, L. D. (2020). AI-enabled future crime. *Crime Science*, *9*(1), 1–13. https://doi.org/10.1186/s40163-020-00123-8

Carville, O. (2021, June 15). Airbnb is spending millions of dollars to make nightmares go away. *Bloomberg*. https://www.bloomberg.com/news/features/2021-06-15/airbnb-spends-millions-making-nightmares-at-live-anywhere-rentals-go-away

CBS News. (2023, September 21). *Airbnb cracking down on fake listings* [Video]. YouTube. https://www.youtube.com/watch?app=desktop&v=vOENIwhP-IE

Corporate Finance Institute (CFI). (2023). *Bait and switch*. https://corporatefinanceinstitute.com/resources/management/bait-and-switch/

Clark, J. (2022, June 29). UK victims lost £1.3bn in 2021 amid surge in online fraud, new data shows. *The Guardian*. https://www.theguardian.com/money/2022/jun/29/uk-victims-lost-13bn-in-2021-amid-surge-in-online-new-data-shows

Clark, J. (2023, May 11). Social media firms should reimburse online fraud victims, say UK bankers. *The Guardian*. https://www.theguardian.com/money/2023/may/11/social-media-firms-should-reimburse-online-fraud-victim-uk-finance

Clark, J., & Wood, Z. (2023, June 16). Victims speak out over 'tsunami' of fraud on Instagram, Facebook and WhatsApp. *The Guardian*. https://www.theguardian.com/technology/2023/jun/16/victims-speak-out-over-fraud-on-instagram-facebook-and-whatsapp

Conti, A. (2019, October 31). I accidentally uncovered a nationwide scam on Airbnb. *Vice*. https://www.vice.com/en/article/43k7z3/nationwide-fake-host-scam-on-airbnb

Cross, C. (2022). Using artificial intelligence (AI) and deepfakes to deceive victims: The need to rethink current romance fraud prevention messaging. *Crime Prevention and Community Safety*, *24*(1), 30–41. https://doi.org/10.1057/s41300-021-00134-w

Cross, C. (2023). Romance baiting, cryptorom and 'pig butchering': An evolutionary step in romance fraud. *Current Issues in Criminal Justice*, *36*(3), 334–346. https://doi.org/10.1080/10345329.2023.2248670

Cudd, G. (2022). *Fiverr scams: What they are & how to avoid them.* Don't Do It Yourself. https://ddiy.co/fiverr-scams-how-to-avoid/

Dartmouth College. (n.d.). *Artificial intelligence coined at Dartmouth*. https://home.dartmouth.edu/about/artificial-intelligence-ai-coined-dartmouth

Dent, S. (2022, July 14). *Uber sued by more than 500 women over sexual assault and kidnapping claims*. Engadget. https://www.engadget.com/uber-sued-by-more-than-500-women-over-rapes-kidnappings-assaults-092733782.html

Ekstein, N. (2023, October 2). Airbnb is fundamentally broken, its CEO says. He plans to fix it. *Bloomberg*. https://www.bloomberg.com/news/articles/2023-10-02/airbnb-is-broken-its-ceo-says-here-are-his-plans-to-fix-it

Eliot, L. (2023, March 1). Generative AI ChatGPT as masterful manipulator of humans, worrying AI ethics and AI law. *Forbes*. https://www.forbes.com/sites/lanceeliot/2023/03/01/generative-ai-chatgpt-as-masterful-manipulator-of-humans-worrying-ai-ethics-and-ai-law/

Fergusson, A. (2021, October 11). *127,183 Airbnb guest complaints expose scams, safety concerns, infestations & more*. Asher & Lyric. https://www.asherfergusson.com/airbnb/

Federal Trade Commission (FTC). (2022). *What to know about romance scams*. Federal Trade Commission Consumer Advice. https://consumer.ftc.gov/articles/what-know-about-romance-scams

Gallagher, L. (2018). *The Airbnb story*. Mariner Books.

García-Peñalvo, F., & Vázquez-Ingelmo, A. (2023). What do we mean by GenAI? A systematic mapping of the evolution, trends, and techniques involved in generative AI. *International Journal of Interactive Multimedia and Artificial Intelligence*, *8*(4), 7–16. https://doi.org/10.9781/ijimai.2023.07.006

Gebbia, J. (2016). *How Airbnb designs for trust* [Video]. TED. https://www.ted.com/talks/joe_gebbia_how_airbnb_designs_for_trust/transcript

Gillespie, E. (2023, January 22). Stranded at sea: Amateur female sailors speak of sexual abuse by captains they met online. *The Guardian*. https://www.theguardian.com/society/2023/jan/23/stranded-at-sea-amateur-female-sailors-speak-of-sexual-abuse-by-captains-they-met-online

Giuffrida, A., & Wilson, A. (2018, September 12). Man jailed in Italy for selling fake TripAdvisor reviews. *The Guardian*. https://www.theguardian.com/world/2018/sep/12/man-jailed-italy-selling-fake-tripadvisor-reviews-promo-salento

Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. *IEEE Access*, *11*, 80218–80245. https://ieeexplore.ieee.org/document/10198233

Hartmans, A. (2017, August 10). Airbnb now has more listings worldwide than the top five hotel brands combined. *Business Insider*. https://www.businessinsider.com/airbnb-total-worldwide-listings-2017-8

Heikkilä, M. (2023, February 7). Why detecting AI-generated text is so difficult (and what to do about it). *MIT Technology Review*. https://www.technologyreview.com/2023/02/07/1067928/why-detecting-ai-generated-text-is-so-difficult-and-what-to-do-about-it/

Helmus, T. C. (2022). *Artificial intelligence, deepfakes, and disinformation. A primer.* RAND. https://www.rand.org/pubs/perspectives/PEA1043-1.html

Hermann, E. (2021). Artificial intelligence and mass personalization of communication content—An ethical and literacy perspective. *New Media & Society*, 24, 1258–1277. https://doi.org/10.1177/14614448211022702

Hill, M. (2023, November 8). Generative AI could erode customer trust, half of business leaders say. *CSO Online*. https://www.csoonline.com/article/1071129/generative-ai-could-erode-customer-trust-half-of-business-leaders-say.html

Holmes, A. (2019, October 25). More than 30 women are suing Lyft, saying the company didn't do enough to protect them from sexual assault and kidnapping. *Business Insider*.https://www.businessinsider.com/lyft-lawsuit-women-claiming-lack-of-sexual-assault-kidnapping-protection-2019-10

Igual, R. (2018, April 3). Stripped & robbed: Another suspected online dating attack in Pretoria. *Mamba Online*. https://www.mambaonline.com/2018/04/03/stripped-robbed-another-online-dating-attack-pretoria

Igual, R. (2023, February 16). Four arrested over "Grindr Gang" attacks. *Mamba Online*. https://www.mambaonline.com/2023/02/16/breaking-four-arrested-over-grindr-gang-attacks/

Isacenkova, J., Thonnard, O., Costin, A., Francillon, A., & Balzarotti, D. (2014). Inside the scam jungle: A closer look at 419 scam email operations. *EURASIP Journal on Information Security*, *2014*(4), 1–18. https://doi.org/10.1186/1687-417X-2014-4

Jain, A. (2017, April 21). *What we're doing to prevent fake listing scams*. Airbnb Newsroom. https://news.airbnb.com/what-were-doing-to-prevent-fake-listing-scams

Jones, R. (2023, September 28). Up to tenth of Amazon shoppers in Great Britain 'bribed' by sellers to offer good review, poll finds. *The Guardian*. https://www.theguardian.com/technology/2023/sep/28/up-to-tenth-of-amazon-shoppers-in-great-britain-bribed-by-sellers-to-offer-good-review-poll-finds

Kennedy, L. (2022, July 4). *How to avoid getting caught up in the pet scam boom.* Choice. https://www.choice.com.au/outdoor/pets/products/articles/pet-scams

Kerr, D. (2019, October 24). Lyft is fostering a sexual assault 'epidemic,' victims say. *CNET*. https://www.cnet.com/tech/mobile/features/lyft-is-fostering-a-sexual-assault-epidemic-victims-say

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Liu, B., Xiao, B., Jiang, X., Cen, S., He, X., & Dou, W. (2023). Adversarial attacks on large language model-based system and mitigating strategies: A case study on ChatGPT. *Security and Communication Networks*, *8691095*, 1–10. https://doi.org/10.1155/2023/8691095

Low, H., & Fakim, N. (2023, May 30). Booking.com guests turning up at family's home in Plumstead. *BBC*. https://www.bbc.com/news/uk-england-london-65726102

Mann, T. (2019, August 21). Friends arrive at £5500 'luxury' Booking.com villa to find nothing but wasteland. *Mirror*. https://www.mirror.co.uk/news/world-news/friends-show-up-5500-luxury-18976743

Marr, B. (2023, May 19). A short history of ChatGPT: How we got to where we are today. *Forbes*. https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/

Marsh, S. (2023, April 22). 'It can be incredibly profitable': The secret world of fake online reviews. *The Guardian*. https://www.theguardian.com/money/2023/apr/22/it-can-be-incredibly-profitable-the-secret-world-of-fake-online-reviews

May, N. (2022, September 5). Losses from 'heart-wrenching' puppy scams increase 1,000% over last two years. *The Guardian*. https://www.theguardian.com/australia-news/2022/sep/05/losses-from-heart-wrenching-puppy-scams-increase-1000-over-last-two-years

McCormick, E. (2023, April 22). Gone in seconds: Rising text message scams are draining US bank accounts. *The Guardian*. https://www.theguardian.com/money/2023/apr/22/robo-texts-scams-bank-accounts

Miller, E. J., Steward, B. A., Witkower, Z., Sutherland, C. A. M., Krumhuber, E. G., & Dawel, A. (2023). AI hyperrealism: Why AI faces are perceived as more real than human ones. *Psychological Science*, *34*(12), 1–14. https://doi.org/10.1177/09567976231207095

Mzekandaba, S. (2023, April 4). Cyber crime's annual impact on SA estimated at R2.2bn. *ITWeb*. https://www.itweb.co.za/content/JN1gPvOAxY3MjL6m

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

Ognyanova, K., Lazer, D., Robertson, R. E., & Wilson, C. (2020). Misinformation in action: Fake news exposure is linked to lower trust in media, higher trust in government when your side is in power. *Harvard Kennedy School Misinformation Review*, *1*(4), 1–19. https://doi.org/10.37016/mr-2020-024

O'Neill, S. (2018, September 12). *A peddler of fake reviews on TripAdvisor gets jail time*. Skift. https://skift.com/2018/09/12/fake-reviews-tripadvisor-jail-italy/

Ooi, K-B., Tan, G. W-H., Al-Emran, M., Al-Sharafi, M. A., Capatina, A., Chakraborty, A., Dwivedi, Y. K., Huang, T-L., Kar, A. K., Lee, V-H., Loh, X-M., Micu, A., Mikalef, P., Mogaji, E., Pandey, N., Raman, R., Rana, N. P., Sarker, P., Sharma, A., Teng, C-I., Wamba, S. F., & Wong, L-W. (2023). The potential of generative artificial intelligence across disciplines: Perspectives and future directions. *Journal of Computer Information Systems*, 1–32. https://doi.org/10.1080/08874417.2023.2261010

Patel, A. (2023, February 14). *Analysis of YouTube USDT crypto scams*. Withsecure. https://labs.withsecure.com/content/dam/labs/docs/WithSecure_Analysis_of_USDT_crypto_scams_on_YouTube.pdf

Roose, K. (2023, May 30). A.I. poses 'risk of extinction,' industry leaders warn. *The New York Times*. https://www.nytimes.com/2023/05/30/technology/ai-threat-warning.html

Ropek, L. (2022, July 23). *What is 'pig butchering,' the crypto scam that's flooding the FBI's phone lines?* Gizmodo. https://gizmodo.com/what-is-a-pig-butchering-crypto-scam-1849316921

Rushing, E. (2020, March 9). A Philly lawyer nearly wired $9,000 to a stranger impersonating his son's voice, showing just how smart scammers are getting. *The Philadelphia Inquirer*.https://www.inquirer.com/news/voice-scam-impersonation-fraud-bail-bond-artificial-intelligence-20200309.html

Sartori, L., & Theodorou, A. (2022). A sociotechnical perspective for the future of AI: Narratives, inequalities, and human control. *Ethics and Information Technology*, *24*(1), 1–11. https://doi.org/10.1007/s10676-022-09624-3

Sekudu, B. (2023, March 13). Joburg LGBTQIA+ community still targeted by "Grindr Gang" after 13 reports of attacks in 8 months. *News24*. https://www.news24.com/life/relationships/dating/joburg-lgbtiq-community-still-targeted-by-grindr-gang-after-13-reports-of-attacks-in-8-months-20230313

Shah, P. (2023, May 12). *Facebook Marketplace's dirty dozen: The 12 most common scams and how to avoid them.* Android Police. https://www.androidpolice.com/avoid-facebook-marketplace-scams/#mailing-items

Sthapit, E., & Björk, P. (2019). Sources of distrust: Airbnb guests' perspectives. *Tourism Management Perspectives*, *31*, 245–253. https://doi.org/10.1016/j.tmp.2019.05.009

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

Stouffer, C. (2022, August 26). *12 Instagram scams to know and avoid in 2023*. Norton. https://us.norton.com/blog/online-scams/instagram-scams#

Temperton, J. (2020, November 2). I stumbled across a huge Airbnb scam that's taking over London. *Wired*. https://www.wired.co.uk/article/airbnb-scam-london

Thomas, T. (2022, March 8). Internet scams to be included in UK online safety bill. *The Guardian*.https://www.theguardian.com/money/2022/mar/08/internet-scams-now-included-in-uk-online-safety-bill

Tripadvisor. (2023). Tripadvisor review transparency report. https://www.tripadvisor.com/TransparencyReport2023

Turkos, A. (2019, September 17). Why I'm suing Lyft. *Medium*. https://aturkos.medium.com/why-im-suing-lyft-6a409e316d1f

UK Finance. (2022). *Over £1.2 billion stolen through fraud in 2022, with nearly 80 per cent of app fraud cases starting online*. https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app

Vahl, S. (2022, 3 August). Booking.com scam: Tourists descend on north London private home. *BBC*. https://www.bbc.com/news/uk-england-london-62407046

Wach, K., Duong, C. D., Ejdys, J., Kazlauskaitė, R., Korzynski, P., Mazurek, G., Paliszkiewicz, J., & Ziemba, E. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. *Entrepreneurial Business and Economics Review*, *11*(2), 7–30. https://doi.org/10.15678/EBER.2023.110201

Walsh, C., Saxena, D., & Muzellec, L. (2020). AirBnB: Managing trust and safety on a platform business. *The Irish Journal of Management*, *39*(2), 126–134. https://doi.org/10.2478/ijm-2020-0004

Walsh, H. (2023, April 21). Facebook fake review groups targeting Amazon, Google and Trustpilot. *Which?* https://www.which.co.uk/news/article/facebook-still-infiltrated-by-fake-review-factories-aTTJ24L5vYyJ

Whitty, M., & Buchanan, T. (2012). *The psychology of the online dating romance scam*. University of Leicester. https://www.scribd.com/document/296206044/The-Psychology-of-the-Online-Dating-Romance-Scam-copypasteads-com

Wood, Z. (2023, June 18). Social media sites failing to curb 'cottage industry' of fake reviews, Amazon says. *The Guardian*. https://www.theguardian.com/money/2023/jun/18/amazon-social-media-platforms-fake-online-reviews

Zamani, E. D., Choudrie, J., Katechos, G., & Yin, Y. (2019). Trust in the sharing economy: The AirBnB case. *Industrial Management & Data Systems*, *119*(9), 1947–1968. https://doi.org/10.1108/IMDS-04-2019-0207

Zawacki-Richter, O., Marín, V., Bond, M., & Gouverneur, F. (2019). Systematic review of research on artificial intelligence applications in higher education – where are the educators? *International Journal of Educational Technology in Higher Education*, *16*(39), 1–27. https://doi.org/10.1186/s41239-019-0171-0