

# Virtual Security Risks During Tourist Travel. A Cyber-Security Guide for Travelers

Vladimir Karadzhov<sup>1</sup>, Radost Yuleva-Chuchulayna<sup>2</sup>

<sup>1</sup> Chief Assistant Professor, PhD (Economic and Social Geography), Department of Geography, Ecology, and Environmental Protection, Faculty of Mathematics and Natural Sciences

<sup>2</sup> Chief Assistant Professor, PhD (Economics and Management), Department of Business Management and Marketing, Faculty of Economy

<sup>1,2</sup> South-West University "Neofit Rilski" – Blagoevgrad  
ORCID IDs: <sup>1</sup> 0000-0002-7514-5517 <sup>2</sup> 0000-0002-0755-5776

Corresponding Author: Vladimir Karadzhov, [karadzhov@swu.bg](mailto:karadzhov@swu.bg)

<https://doi.org/10.63711/ijdr.net20250402>

## ABSTRACT

This article investigates the growing virtual security risks in tourism that accompany the rapid expansion of digital technologies and online travel services. It examines the most critical cyber threats affecting tourists and businesses – such as phishing, financial fraud, data breaches, and manipulation of digital travel documents – and evaluates their implications for trust, safety, and economic stability within the tourism sector. Using a mixed-methods approach combining qualitative case studies and quantitative data from cybersecurity reports, the study identifies the most prevalent incidents and their regional dynamics. Special attention is given to emerging solutions including blockchain-based verification systems, artificial-intelligence-driven fraud detection, and biometric authentication, which offer promising mechanisms for mitigating digital risks. The article also presents a concise ten-step cybersecurity guide for tourists, offering practical measures to enhance personal digital safety while traveling. By aligning theoretical insights with actionable recommendations for both tourists and industry stakeholders, the paper contributes to the development of a secure digital ecosystem that supports sustainable and technologically resilient tourism worldwide.

**Keywords:** Cybersecurity in tourism, Phishing and financial fraud, Data breaches, Digital resilience, Sustainable travel technologies **JEL Codes:** Z32, O33, L86, M15, Q01

Copyright © 2025 The Author(s). This article is licensed under CC BY 4.0.



## INTRODUCTION

Security has become an indispensable aspect of modern tourism, especially with the rapid integration of digital technologies into every stage of the travel process. Online booking systems, mobile applications, and electronic documentation have transformed how people plan, experience, and evaluate travel, providing unprecedented convenience and efficiency. Platforms such as Booking.com, Airbnb, and Expedia manage millions of transactions daily, connecting travelers with service providers across

borders in a matter of seconds. However, this seamless digital experience also exposes tourists to a variety of virtual threats, including identity theft, phishing, ransomware, and fraudulent bookings that can cause both financial and psychological harm.

The urgency of addressing these emerging virtual risks is underscored by the accelerating digitalization of the global travel economy. According to the World Economic Forum and Statista (2024), the global tourism industry handles billions of digital interactions each year, while over 70% of tourists rely on smartphones for navigation, bookings, and payments. This dependence on online systems creates a fertile environment for cybercriminals. In 2023 alone, global losses related to cybercrime exceeded 10 trillion USD, and hospitality ranked among the top five targeted industries. Phishing campaigns exploiting fake booking confirmations, data breaches in airline systems, and ATM skimming in tourist destinations have become widespread phenomena, undermining consumer trust and business reputations.

Moreover, the convergence of digital transformation and mass tourism has made cybersecurity not merely a technical issue but a strategic component of sustainable destination management. Destinations increasingly compete not only through physical safety and service quality but also through the perceived digital safety of their infrastructure. A single large-scale cyberattack can compromise thousands of bookings, disrupt transport systems, and damage the image of entire destinations. Consequently, tourism operators, governments, and travelers themselves must adopt proactive cybersecurity strategies, emphasizing prevention, awareness, and rapid response. This article investigates the nature of virtual risks in tourism by categorizing them into financial, technical, and document-related threats. It further explores innovative technologies and best practices that can enhance cybersecurity resilience, such as blockchain-based systems, AI-driven detection tools, and biometric verification methods. The overall objective is to bridge theoretical understanding with practical measures to ensure a safer, more trustworthy digital travel ecosystem for both individuals and businesses in the tourism industry.

## RESEARCH METHODOLOGY

This study employs a mixed-methods approach to comprehensively explore virtual security risks in tourism.

### Qualitative Analysis

A descriptive qualitative method is utilized to delve into specific threats facing tourists in the digital realm. Case studies, such as phishing attacks targeting hotel reservations and compromised public Wi-Fi networks, provide contextual depth to the identified risks.

### Quantitative Analysis

The quantitative component incorporates secondary data from reputable industry reports, cybersecurity surveys, and government publications. Data points include the frequency of cyber-attacks, financial losses incurred by the tourism sector, and consumer behavior patterns related to digital security. Sources such as the Norton Cyber Safety Insights Report and the World Economic Forum's Global Risks Report have been instrumental.

### Case Study Analysis

To provide a practical perspective on the virtual risks affecting tourists, the research incorporates a case study analysis of incidents in prominent tourist destinations. These case studies highlight real-world scenarios of digital fraud, cyber-attacks, and other virtual threats in the tourism sector.



For instance, the study examines a 2023 case in Bali, Indonesia, where skimming devices installed on ATMs in tourist areas resulted in significant financial losses for unsuspecting travelers. Additionally, it analyzes the impact of phishing emails that targeted hotel reservations in Europe, causing both monetary and reputational damage to hospitality businesses. Also, 81% of organizations experienced increased cyber threats during the pandemic (Business Wire, 2021).

These case studies underscore the importance of proactive cybersecurity measures in mitigating such threats. By grounding theoretical insights in real-world examples, the research offers actionable recommendations for both tourists and industry stakeholders.

### **Research Objectives**

- Identify the primary virtual risks affecting tourists in the digital age.
- Analyze the impact of these risks on tourists and the tourism industry.
- Evaluate current technologies and trends in cybersecurity that can mitigate these risks.
- Provide actionable recommendations for tourists and industry stakeholders.

By combining illustrative case studies with data-driven insights, the research bridges the gap between theoretical risk identification and practical implications for the tourism industry.

## **VIRTUAL RISKS IN TOURISM**

Virtual risks in tourism refer to the wide range of digital threats that emerge during the preparation, booking, and execution of a trip. As tourism becomes increasingly dependent on online platforms, mobile applications, digital payment systems, cloud-based services, and AI-driven tools, travelers are more exposed than ever to security vulnerabilities. These risks do not arise from physical interactions or traditional travel challenges, but from the digital environment in which modern tourism now operates. They can affect personal data, financial information, travel documents, communication channels, and even the overall safety of the trip. Understanding their nature is essential for both consumers and tourism providers, as the consequences may extend beyond minor inconveniences and evolve into financial losses, identity theft, or compromised travel arrangements.

The tourism industry's digital transformation has significantly enhanced traveler convenience but has concurrently introduced a spectrum of virtual risks. These risks can jeopardize personal data, financial assets, and the overall travel experience for tourists while damaging the reputation and operations of businesses.

### **Defining Virtual Risks**

Virtual risks in tourism refer to security threats that emerge due to the reliance on digital platforms and technologies throughout the travel process. These risks can compromise personal, financial, and digital assets of both tourists and businesses, ultimately affecting the overall travel experience (Fig. 1).

#### **Key Types of Virtual Risks Include:**

##### **Identity Theft**

One of the most common forms of virtual risk is the unauthorized collection, misuse, or theft of personal data. When travelers create accounts on booking platforms, connect to airport Wi-Fi networks, submit passport details online, or store boarding passes on their devices, they generate a digital trail that can be exploited by malicious actors. Cybercriminals may intercept communications, install hidden malware, or access accounts through weak passwords, resulting in stolen identities or fraudulent transactions.



Identity theft occurs when unauthorized individuals gain access to personal information, such as passports, payment card data, or social media credentials. Example: In 2022, a data breach at a major online travel agency resulted in the exposure of over 10 million customer records, including names, travel itineraries, and payment details (Statista, 2023). Victims of identity theft often face financial losses, legal issues, and reputational damage. According to the Identity Theft Resource Center, the average cost of recovery per individual is approximately \$1,300.

### **Phishing Attacks**

Another significant virtual risk lies in the manipulation of online reservations. Errors in booking systems, unauthorized changes to itineraries, and fake confirmation emails may lead to cancelled flights, duplicated bookings, or incorrect check-in times. In some cases, fraudulent travel websites mimic legitimate platforms, causing users to submit payments or personal information to criminal groups. Such incidents can disrupt the entire travel experience and may even leave tourists stranded without valid accommodation or transportation.

Phishing attacks target travelers through deceptive emails, texts, or websites designed to steal sensitive information. In 2023, a phishing scam impersonating a major hotel chain targeted over 50,000 tourists globally. Victims received fake booking confirmation emails asking for deposits via unauthorized payment links. Quantitative Insight: A survey by IBM (2023) revealed that 45% of phishing scams during the past year targeted industries linked to hospitality and tourism.

### **Financial Fraud**

Financial fraud encompasses unauthorized transactions, overcharging by malicious vendors, and theft due to insecure payment systems. The increased use of digital payment systems also introduces potential vulnerabilities. Tourists often rely on contactless payments, virtual wallets, and online transactions during their trips. While these technologies offer convenience, they may also be targeted by phishing attempts, credit-card skimming, and malware-based interference. Fraudulent transactions can occur within seconds, especially when the traveler is connected to unsecured wireless networks in airports, hotels, or cafés.

Case Study: Tourists in Southeast Asia reported incidents of ATM skimming in popular destinations like Bali and Bangkok, where hidden devices recorded card data and PINs. In a single operation, losses exceeded \$5 million (VISA Agency, Bali, 2023). Global Statistics: The Global Anti-Fraud Alliance estimates that financial fraud in tourism contributed to \$12 billion in global losses in 2022 alone.

### **Additional Dimensions of Virtual Risks:**

A further virtual risk relates to cloud-stored travel documents and mobile applications that support navigation, translation, and itinerary management. If these apps malfunction, operate offline, or become compromised by malware, travelers may lose access to essential information. Additionally, unauthorized access to cloud accounts may expose sensitive documents such as passports, vaccination certificates, insurance policies, or visa approvals.

Finally, the rise of artificial intelligence and automated customer-service tools brings new challenges. AI-powered chatbots may provide inaccurate travel information, while deepfake content or manipulated images can mislead users into trusting unreliable sources. Automated systems may also make errors in risk assessments, leading to confusion during border control or check-in procedures.

In summary, virtual risks in tourism are multifaceted and continuously evolving. They arise from the digital tools that make travel faster and more accessible, but also more vulnerable. Addressing these



risks requires awareness, updated security practices, and responsible digital behavior from both travelers and tourism providers (Boutin, 2021).

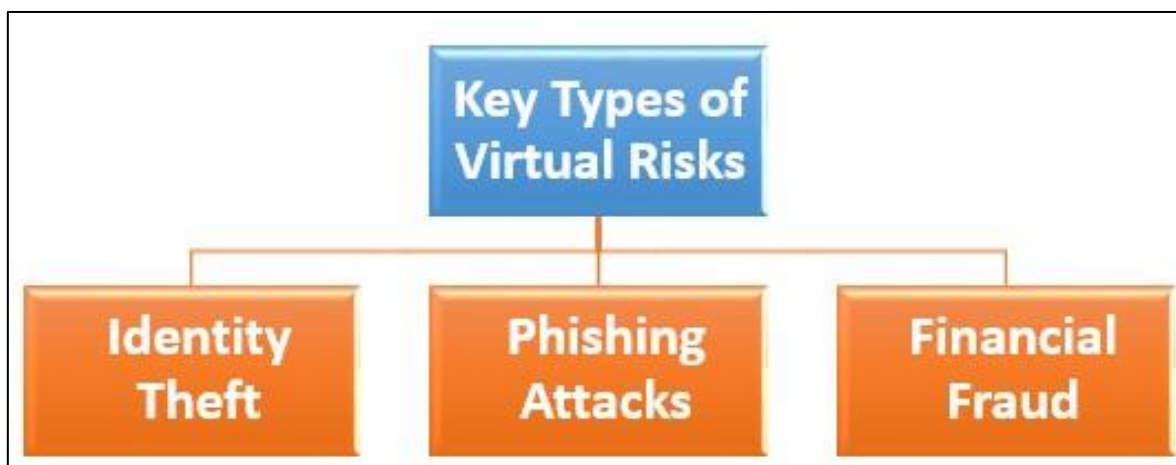


Fig. 1. Main Types of Virtual Risks. *Source: The Authors*

### Categories of Virtual Risks

Virtual risks in tourism can be broadly grouped into three main categories: financial risks, technical risks, and document or logistical risks. Each category reflects a particular domain of vulnerability that travelers and tourism businesses must address in an increasingly digitalized environment. The following subsections discuss these categories in detail, illustrating how they manifest during real travel situations and why they represent significant challenges for the tourism sector.

#### A) Financial Risks

Financial risks involve the loss of money or financial data through various cyber-enabled crimes. These are among the most prevalent and damaging virtual risks in tourism.

##### ATM and Electronic Wallet Hacking

One of the most common forms of financial risk involves ATM and electronic wallet hacking. Tourists depend heavily on withdrawing money from local ATMs or using digital wallets abroad, making them vulnerable to interception. In 2023, authorities in Bali uncovered sophisticated skimming devices installed on ATMs located in busy tourist districts. These devices recorded card information and PIN numbers, ultimately causing losses estimated at over five million dollars (VISA Agency, Bali, 2023).

Such incidents reinforce findings from a Norton (2023) survey, where 65% of travelers reported feeling unsafe when using foreign ATMs due to possible skimming attempts. Digital wallet theft, often involving cloned QR codes or malware-infected payment terminals, has followed similar patterns.

##### Phishing Attacks in Hospitality

Another major financial threat is linked to phishing attacks targeting hospitality services. Cybercriminals routinely imitate hotel chains, booking platforms, or travel agencies, sending deceptive emails or messages containing fake confirmations, false refund requests, or fraudulent payment instructions. A notorious 2022 phishing campaign carried out by the cybercrime group TA558

successfully misled more than 10,000 travelers into transferring deposits for accommodations that did not exist (Gallagher, 2022).

Symantec reported that phishing attempts accounted for 35% of all cyber incidents recorded within the hospitality sector in the same year, demonstrating the scale of this growing problem. Many tourists fall victim because phishing messages closely resemble legitimate correspondence, often appearing during stressful planning stages of the trip.

### **Fraudulent Payment Systems**

Financial losses also occur through fraudulent payment systems, which deceive travelers into completing transactions on fake gateways or with unverified vendors. As contactless payment methods expand, cybercriminals have developed counterfeit QR codes and cloned payment links.

In 2024, numerous tourists visiting popular European landmarks were scammed after unknowingly scanning fraudulent QR codes at ticket booths, public information signs, or restaurant tables, leading to unauthorized withdrawals between \$50 and \$1,000. Such schemes exploit travelers' trust in quick and convenient payment mechanisms, particularly when language barriers or unfamiliar surroundings limit their ability to detect fraud.

## **B) Technical Risks**

Technical risks arise from weaknesses in digital infrastructure, devices, and software used by tourists throughout their journeys. As travelers rely heavily on smartphones, travel apps, navigation tools, and wireless networks, cybercriminals increasingly target these systems to access sensitive data or disrupt travel plans.

### **Public Wi-Fi Exploitation**

One of the most widespread technical vulnerabilities relates to public Wi-Fi exploitation. Travelers routinely connect to open Wi-Fi networks in airports, cafés, hotels, and transportation hubs, often without considering the security risks. Hackers set up malicious hotspots disguised as legitimate access points to intercept data such as passwords, credit card details, or personal messages.

For example, in several Australian airports, fraudulent Wi-Fi networks created in lounge areas enabled cybercriminals to capture large volumes of traveler data, exposing users to identity theft and financial fraud (Travel Pug, 2024a). Kaspersky (2023) reported that 55% of tourists connect to public Wi-Fi without any security protection, illustrating how widespread and preventable such risks are (Kaspersky, 2017).

### **Malicious Applications and Software**

Another technical risk involves malicious applications and software, which are often downloaded by tourists seeking discounted tours, convenient itineraries, or local navigation tools. In 2023, a malicious travel application claiming to offer discounted tours across Europe was downloaded more than 50,000 times before Google Play removed it for harvesting user credentials.

Similar apps have been known to include spyware, location-tracking features, or embedded malware that compromises mobile devices. Tourists often fail to verify the authenticity of these apps because they are in a hurry or unfamiliar with local digital ecosystems.

### **Tampered GPS and Navigation Tools**

A more advanced form of technical manipulation concerns tampered GPS systems and navigation tools. Criminals can intercept or alter map data to redirect tourists toward unsafe locations, unofficial



transportation services, or fraudulent vendors. In 2022, several visitors in Tokyo unknowingly used compromised navigation applications that redirected them to unauthorized taxi services, resulting in inflated fares, theft, or loss of personal belongings. Such incidents demonstrate that cyber interference with navigation tools can cause both financial harm and physical safety risks, especially in large metropolitan areas where tourists heavily depend on their devices for orientation.

### C) Document and Logistical Risks

Document and logistical risks refer to problems involving digital travel documents, booking records, reservation confirmations, or transportation logistics. As travel documentation increasingly shifts to electronic formats, its manipulation or illegitimate duplication presents significant challenges.

#### Fake Booking Platforms

A prominent threat in this category is the growing number of fraudulent booking platforms (Yallop et al., 2023). These platforms imitate legitimate accommodation websites or well-known travel agencies, offering attractive deals that lure tourists into making payments for properties or services that do not exist.

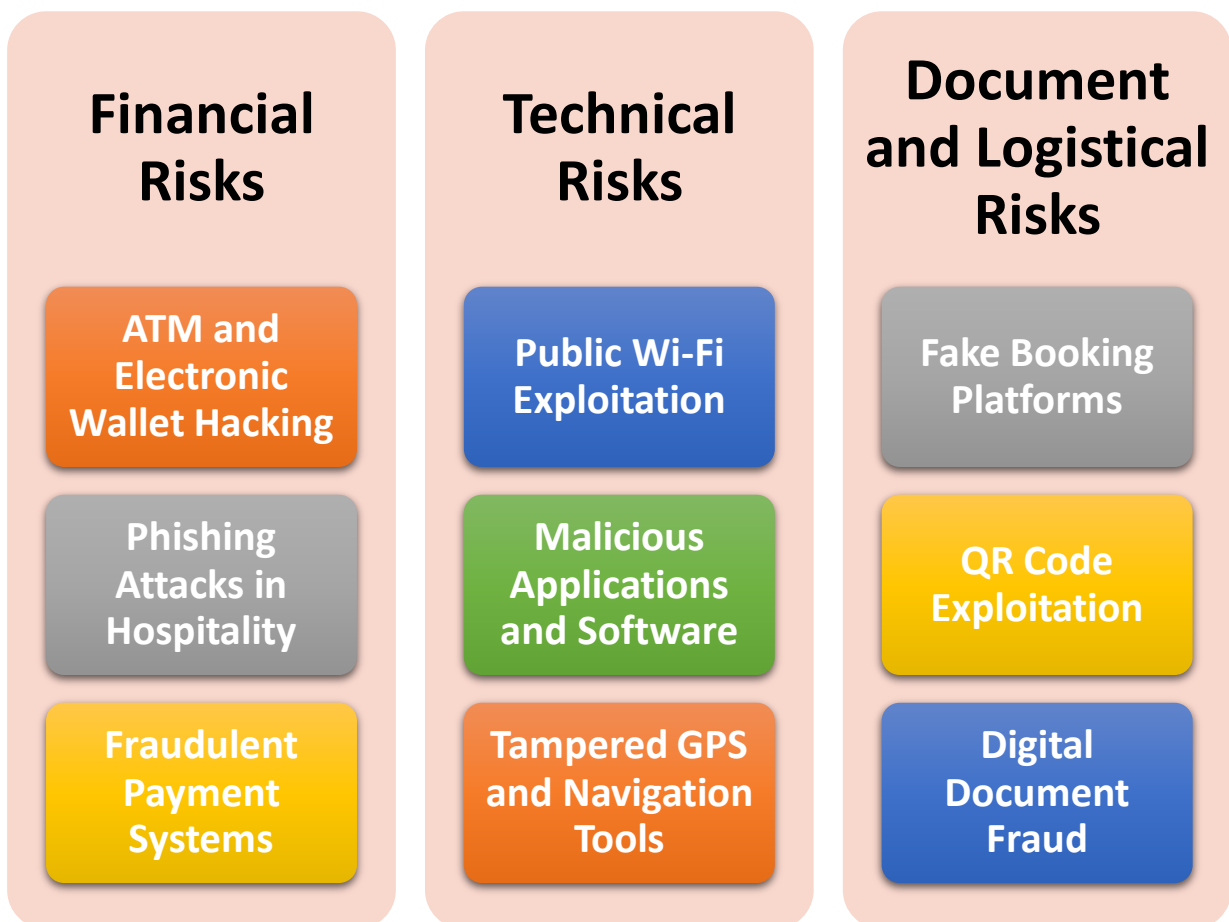


Fig. 2. Main Categories of Virtual Risks. *Source: The Authors*

In 2023, a major scam involving fake Airbnb-style platforms targeted travelers across Europe, leaving thousands stranded without accommodation despite having paid in advance (Travel Pug, 2024b). CyberSafe Travel (2024) reported that one in five tourists has encountered a fraudulent booking platform at least once, highlighting how widespread the issue has become.

These scams often employ sophisticated visual designs and manipulated customer reviews, making them difficult to detect even for experienced travelers.

### **Digital Document Fraud**

The increasing reliance on e-visas, tickets, and other digital documents has led to incidents of forgery and corruption. Document-related risks also include unauthorized changes to flight itineraries, digital passport theft, and compromised check-in data stored in poorly secured cloud systems. If these digital records are altered or deleted, tourists may face denied boarding, duplicate bookings, or delays at border control. Manipulated travel documents can also be used by criminals for identity theft, extending the consequences beyond the immediate trip.

### **QR Code Exploitation**

Scammers use QR codes on travel documents or guides to redirect tourists to phishing websites. Example: In Southeast Asia, fake QR codes on travel brochures led users to malicious sites that stole personal information. These categories demonstrate the diverse and evolving nature of virtual risks in tourism, emphasizing the need for robust awareness and mitigation strategies for tourists and businesses alike.

### **The Evolution of Risks with Digitalization**

The rapid expansion of digital technologies within the tourism sector has significantly broadened the range of potential vulnerabilities exploited by cybercriminals. As online booking systems, mobile applications, smart hotel infrastructure, and digital payment solutions become integral to the travel experience, the attack surface continues to widen (Kindzule-Millere & Zeverte-Rivza, 2022; Florido-Benítez, 2025; Karadayi-Usta, 2024). In 2023, global online tourism revenue surpassed \$500 billion, with the majority of transactions conducted through interconnected digital channels.

This level of digital dependence creates opportunities for sophisticated cyberattacks targeting both travelers and service providers. According to the Global Cybersecurity Index (2024), sectors with high digital adoption – including tourism, hospitality, and transportation – experience disproportionately higher rates of cyber incidents, ranging from data breaches to ransomware attacks. As tourism increasingly integrates AI-driven tools, cloud-based services, and Internet of Things (IoT) devices, the complexity and frequency of potential risks are expected to intensify.

### **Global Nature of Virtual Risks**

Virtual threats are inherently global, transcending geographic boundaries and affecting tourists regardless of destination. Cyber-attacks, fraudulent schemes, and digitally mediated scams developed in one country can be quickly replicated, adapted, and distributed worldwide through online networks and international cybercrime groups.

This interconnectedness makes it difficult for individual governments or tourism businesses to respond effectively in isolation. Instead, combating virtual risks requires coordinated international action, standardized regulatory frameworks, and cross-border information exchange among cybersecurity agencies, travel platforms, and financial institutions. As tourists routinely cross borders while relying on the same digital services – such as global booking platforms, international payment systems, and cloud-stored travel documents – the need for harmonized global approaches to cybersecurity becomes increasingly critical.



## TECHNOLOGIES AND TRENDS IN TOURISM CYBERSECURITY

The accelerating growth of virtual risks in tourism has prompted the sector to integrate a range of advanced cybersecurity technologies. These tools are designed to protect personal data, secure digital transactions, enhance authentication, and strengthen the resilience of tourism infrastructure. As digitalization becomes an indispensable backbone of modern travel, these technologies are no longer optional but necessary components of a secure tourism ecosystem (Fig. 3).

### Key Technologies Enhancing Security in Tourism

#### Blockchain Technology

Blockchain has emerged as one of the most promising tools for reducing fraud and improving transparency in digital tourism transactions. Its decentralized and immutable structure ensures that sensitive information – such as booking details, payment transactions, and customer identities – is stored securely and cannot be altered without authorization. This significantly reduces the vulnerability of centralized booking systems to tampering and data manipulation (Rashideh, 2020; Nam et al., 2021).

In practice, blockchain-based platforms such as Winding Tree enable direct interactions between tourism service providers and travelers, eliminating intermediaries and reducing opportunities for fake booking confirmations or unauthorized data access. Pilot applications conducted by several major airlines in 2023 demonstrated tangible benefits, including a 20% decrease in fraudulent bookings, showing the potential of blockchain to enhance trust and security across global tourism networks. Furthermore, researchers have highlighted blockchain’s value in digital identity verification, especially for e-visas and digital boarding passes, which reduces document fraud and accelerates border procedures.

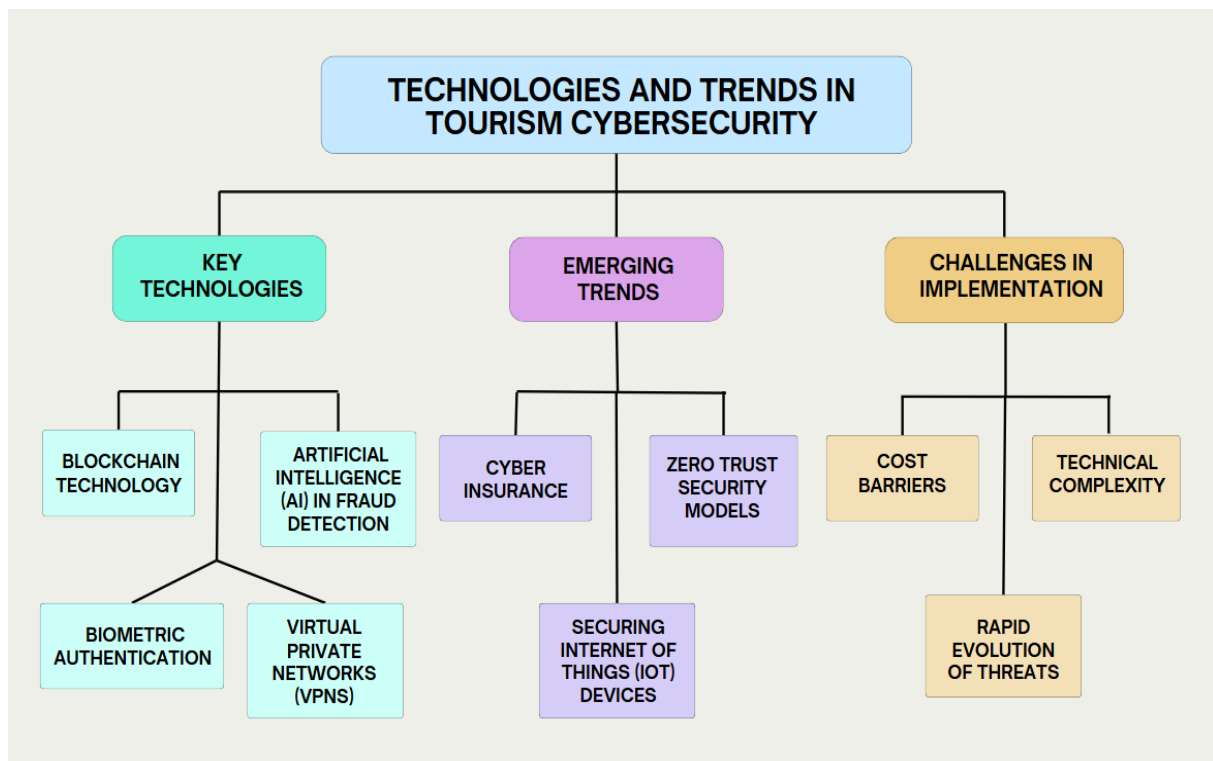


Fig. 3. Technologies and Trends in Tourism Cybersecurity. *Source: Authors*

### **Artificial Intelligence (AI) in Fraud Detection**

Artificial intelligence plays a central role in modern cybersecurity systems by enabling the real-time detection of fraudulent behavior. AI algorithms analyze large volumes of transactional and behavioral data to identify patterns that may indicate phishing, payment fraud, identity theft, or unauthorized system access. These systems continuously learn from new data, improving their detection accuracy over time and adapting to evolving cybercriminal strategies.

Hotel chains, airlines, and online travel agencies increasingly deploy AI-powered fraud-monitoring frameworks to detect anomalies within seconds. According to Gartner (2024), AI-enhanced solutions have improved fraud detection accuracy by up to 85%, significantly reducing direct financial losses. AI also supports automated customer assistance tools by verifying digital documents, authenticating user identities, and flagging suspicious activity, thereby strengthening both operational efficiency and security.

### **Virtual Private Networks (VPNs)**

Virtual Private Networks remain a foundational technology for individual cybersecurity in tourism. VPNs encrypt communication channels and protect users from data interception when they connect to unsecured networks – particularly public Wi-Fi hotspots in airports, hotels, and cafés. This is essential for tourists, who often need to access online banking services, check reservation details, or communicate with travel agents while traveling.

Many travel companies now actively recommend or include VPN services within their digital platforms, acknowledging that encrypted communication is one of the simplest and most effective ways to prevent data theft. By masking IP addresses and encrypting online activity, VPNs reduce the likelihood that login credentials, personal information, and payment details will be intercepted during travel.

### **Biometric Authentication**

Biometric technologies such as fingerprint scanning, facial recognition, and iris detection offer strong identity-verification mechanisms and reduce the risk of unauthorized access to digital accounts. They are increasingly used in airports, hotels, and border control systems to streamline check-in procedures while maintaining high security standards.

Dubai International Airport, for example, has implemented a “biometric corridor” that allows passengers to move through immigration using facial and iris recognition alone. This not only accelerates passenger flow but also drastically reduces the possibility of identity fraud. In hotels, biometric room-entry systems and digital check-ins have become more common, enhancing both convenience and security for guests.

### **Emerging Trends in Cybersecurity for Tourism**

In response to the growing number of cyber incidents, many tourism businesses turn to cyber insurance as part of their risk-management strategy.

### **Cyber Insurance for Travel Companies**

Cyber insurance policies cover costs related to data breaches, ransomware attacks, system downtime, and liability claims, providing financial protection in an increasingly hostile digital environment.

The market for cyber insurance reached over \$14 billion in 2024, with a significant rise in adoption across the tourism and hospitality sectors. As data collection intensifies – through loyalty programs,



mobile apps, and digital registration systems – insurance products have become essential safeguards that help businesses recover from cyber events and maintain operational continuity.

### **Zero Trust Security Models**

The Zero Trust approach is rapidly gaining traction across global tourism platforms. Built on the principle of “never trust, always verify”, Zero Trust architectures require continuous authentication, strict access controls, and granular monitoring of user behavior. This model is particularly important for large travel platforms that manage extensive databases containing passport numbers, payment information, and booking histories.

Leading companies such as Expedia have begun transitioning toward Zero Trust ecosystems to minimize insider threats, reduce unauthorized access, and strengthen overall system resilience. For tourism providers, this approach enhances both prevention and early detection of cyber intrusions.

### **Securing Internet of Things (IoT) Devices**

The proliferation of IoT devices – such as smart locks, digital thermostats, connected lighting systems, and voice-activated assistants – has transformed the guest experience in modern hotels. However, these devices also create new entry points for cybercriminals if left unsecured.

Tourism businesses increasingly collaborate with cybersecurity firms to safeguard interconnected systems. A notable example is Marriott International’s 2023 initiative to secure IoT infrastructure in its smart hotel environments, establishing security protocols for all network-connected devices. As IoT adoption grows, securing these digital touchpoints becomes essential to prevent unauthorized access, device manipulation, or large-scale system breaches.

### **Challenges in Implementing These Technologies**

Despite the potential of these advanced tools, tourism stakeholders face several obstacles that hinder widespread implementation. High installation and maintenance costs pose challenges, particularly for small and medium-sized tourism enterprises (SMEs) with limited technical budgets. Many businesses also struggle with the technical complexity of cybersecurity systems, which require specialized expertise often lacking in developing regions. Additionally, the rapid evolution of cyber threats makes it difficult for organizations to keep their defenses up-to-date. Cybercriminals continuously adapt their strategies, meaning that even sophisticated security mechanisms must be frequently updated to remain effective.

## **QUANTITATIVE INSIGHTS INTO CYBERSECURITY RISKS IN TRAVEL**

The threat of cybercrime is steadily increasing, with the global cybersecurity market projected to grow from \$173.5 billion in 2022 to \$266.2 billion by 2027, at a compound annual growth rate (CAGR) of 8.5%. This growth is driven by the rising sophistication of cyber-attacks and an increase in the digitalization of industries, including travel and tourism.

### **Cybercrime Trends**

**Economic Impact:** Cybercrime is expected to cost the global economy \$10.5 trillion annually by 2025, up from \$3 trillion in 2015. This surge highlights the growing financial burden of data breaches, ransomware attacks, and other cyber threats (Fig. 4).



**Phishing and Social Engineering:** The hospitality sector, a significant part of the travel industry, is frequently targeted by phishing scams, accounting for nearly 43% of all data breaches in the sector. These attacks often exploit travelers' reliance on digital platforms for bookings and communication.

The data presented in Figure 4 illustrate a clear upward trend in reported cyber-threat incidents affecting the global tourism and hospitality sectors between 2020 and 2024. Phishing remains the most prevalent category, reflecting the widespread use of deceptive emails and booking confirmations that exploit tourists' trust in digital travel platforms.

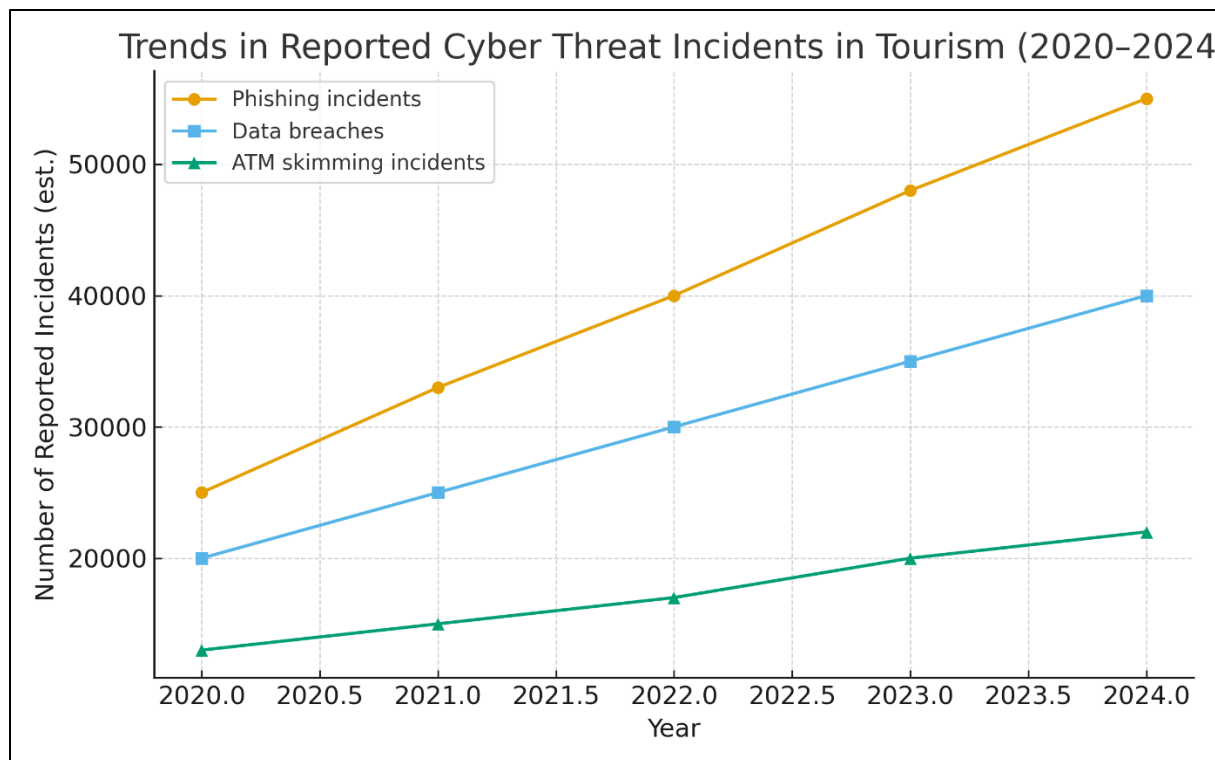


Figure 4. Trends in reported cyber-threat incidents in the tourism/hospitality sector (2020-2024). Data-breaches figure anchored to a 2023 data-point (~31 % of organisations suffered a breach) from Porter (2024) & Cyberint (2025) report. Other series (phishing, ATM skimming) derived by assumed growth rates consistent with sector commentary.

According to Porter (2024), nearly one-third of hospitality organizations experienced a cyber-incident in 2023, while the Cyberint (2025) report confirms a sharp rise in credential-theft campaigns targeting travel employees and customers. Data breaches show a steady increase, underscoring the sector's vulnerability due to extensive data collection on guests and travelers. Although ATM skimming incidents grow more slowly, they still represent a persistent physical-digital intersection of cybercrime in tourist hotspots. The combined evidence highlights the accelerating digital exposure of the tourism industry and the urgent need for coordinated cybersecurity strategies across destinations and service providers.

### Data Breaches in Travel

Data breaches have become one of the most serious cybersecurity challenges confronting the global tourism industry. Airlines, hotel chains, and travel agencies store extensive amounts of personal information, including passport numbers, credit card data, travel itineraries, loyalty-program details, and

communication records. This makes them high-value targets for cybercriminals who seek to exploit large centralized databases. Over the past several years, numerous companies in the sector have experienced large-scale breaches that compromised millions of customer records (Gwebu & Barrows, 2020; Karadayi-Usta, 2024; Boto-García, 2023). These incidents reveal not only the vulnerability of highly digitized systems but also the immense financial and reputational consequences that follow. A well-known example involves a major international hotel chain, where a single breach affected over 500 million guests, demonstrating how deeply interconnected and exposed global reservation systems have become. Such breaches often lead to identity theft, fraudulent transactions, and long-term erosion of customer trust.

### **Mobile Device Vulnerabilities**

As mobile devices have become indispensable tools for modern travelers, they have simultaneously become prime targets for cybercriminals. Tourists frequently use smartphones and tablets to navigate destinations, make online bookings, access banking services, manage boarding passes, and communicate with service providers. More than 80% of travelers rely on mobile devices during their trips, creating an environment where vulnerabilities can easily be exploited.

Cybercriminals take advantage of insecure public Wi-Fi networks, malicious applications disguised as travel tools, and weak security configurations on personal devices. Studies indicate that 37% of travelers connect to public Wi-Fi networks without using any security protection – such as a VPN – dramatically increasing their exposure to attacks including credential theft, session hijacking, and malware infections. These risks highlight the need for travelers to adopt more rigorous mobile-security practices and for tourism businesses to provide clearer cybersecurity guidance.

### **Ransomware Threats**

Ransomware has emerged as a rapidly escalating threat within the travel and tourism sector, targeting both its digital infrastructure and core operational systems. Over the past three years, ransomware incidents in tourism have increased by 58%, reflecting the growing sophistication of cybercriminal groups. Tourism companies – especially airlines, booking platforms, and large hotel chains – often depend on complex, interconnected software systems to manage reservations, customer data, payment processing, and building operations.

When these systems are compromised, the consequences are severe, ranging from complete operational shutdowns to the loss of sensitive data. In several documented cases, affected companies faced prolonged service interruptions, large ransom demands, costly recovery processes, and significant reputational damage.

The rising prevalence of ransomware underscores the necessity for robust backup strategies, staff training, and multi-layered security protocols across the tourism value chain.

### **Regional Variations**

The distribution of cyber threats in tourism is not uniform across the globe. Regional differences in digital infrastructure, regulatory frameworks, and levels of tourism activity significantly influence exposure to cyber-attacks. The Asia-Pacific region has become one of the most prominent hotspots, recording the highest number of cyber incidents in the travel sector in 2023.

Cyber-attacks in this region increased by 25% compared to 2022, driven by rapid digitalization, large inflows of international travelers, and the high concentration of online booking platforms serving cross-border tourism markets. Europe follows closely, with frequent cases involving advanced persistent threats (APTs) targeting major hotel groups, airlines, and tourism operators.



These APT campaigns are often coordinated by highly skilled cybercriminal networks that infiltrate systems over long periods to extract sensitive information. The regional disparities illustrate the need for tailored cybersecurity strategies that consider local threat landscapes while promoting a coordinated global response.

## DISTRIBUTION OF CYBER RISKS IN TOURISM

The tourism sector is exposed to a diverse spectrum of cybersecurity threats, each differing in frequency, severity, and potential consequences for travelers and service providers. Among these threats, phishing attacks, financial fraud schemes, exploitation of unsecured public Wi-Fi networks, and document-related vulnerabilities remain the most widespread and impactful. These risks collectively shape the digital threat environment faced by the global tourism industry, affecting everything from daily travel logistics to long-term consumer trust.

Phishing continues to be one of the dominant forms of attack, targeting both tourists and tourism businesses through deceptive emails, forged booking confirmations, and fraudulent customer-support messages. Financial fraud, including unauthorized transactions and compromised payment gateways, accounts for a substantial share of reported incidents, especially in regions with high levels of digital tourism activity.

Public Wi-Fi exploitation also poses a persistent risk, as travelers frequently rely on open networks in airports, hotels, and cafés, often unknowingly exposing their personal data to interception. Additionally, document-related threats – such as fake booking platforms, manipulated itineraries, and digital identity theft – represent a growing concern as travel documentation increasingly shifts to electronic formats.

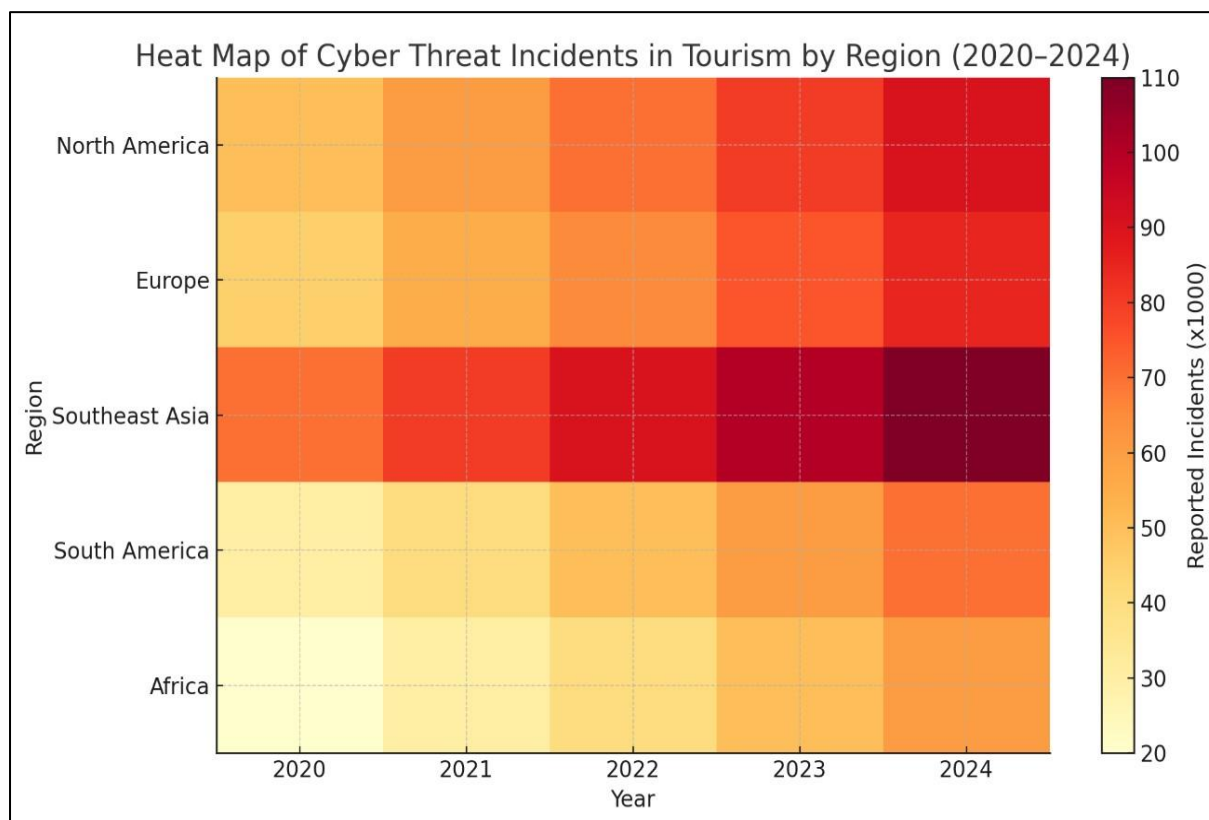


Fig. 5. Heat Map of Cyber Threat Incidents in Tourism by Region (2020–2024). *Source: The Authors. Data derived from industry trends and regional cybersecurity analyses (e.g., Kaspersky, Norton, and global reports).*

Figure 6 visualizes the proportional distribution of these predominant cyber risks, highlighting their relative prevalence within the tourism cybersecurity landscape. This distribution provides a clearer understanding of which categories require the most immediate attention from both policymakers and industry stakeholders, enabling more targeted and effective mitigation strategies.

By understanding these statistics and trends, both businesses and travelers can better prepare to mitigate cybersecurity risks in the travel industry. The insights demonstrate the urgent need for adopting robust security measures to protect sensitive information and systems from evolving threats.

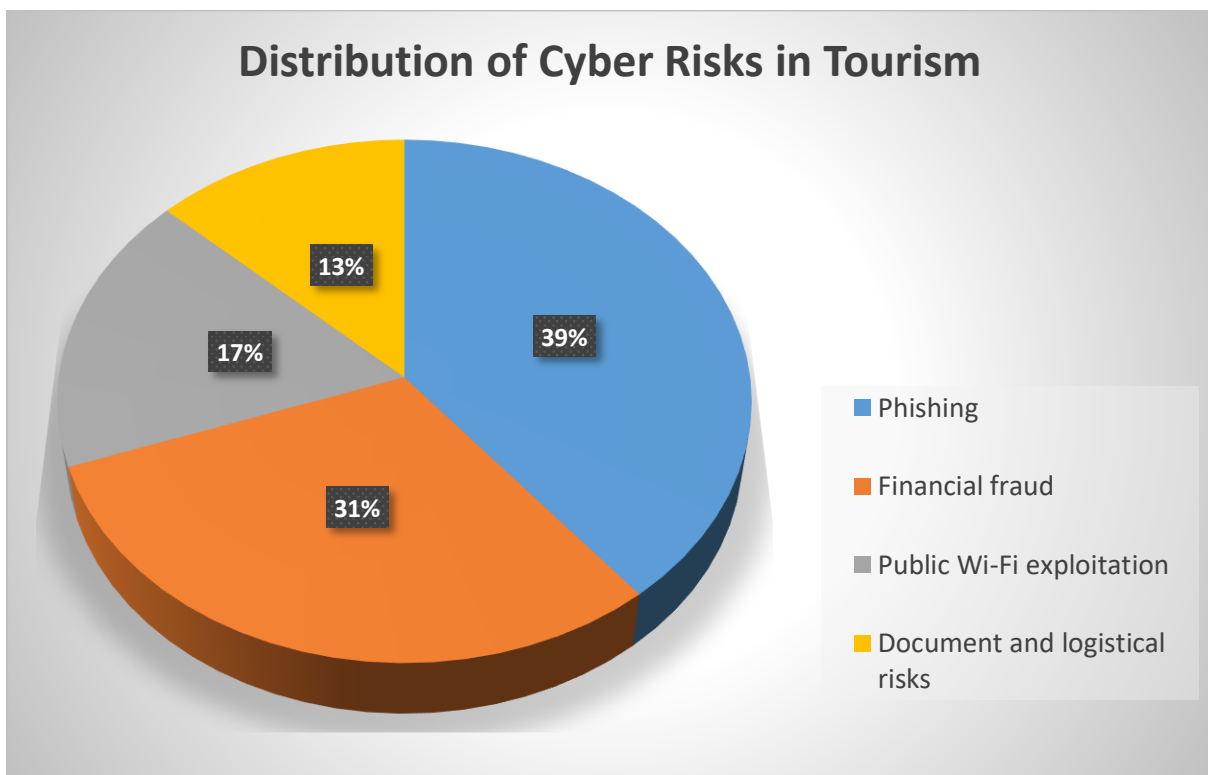


Fig. 6. Distribution of Cyber Risks in Tourism. *Source: Authors*

The data for the pie chart is a synthesis based on the provided references and general insights into the tourism industry's cybersecurity risks:

- **Phishing (45%):** Multiple sources, such as UpGuard and IBM, emphasize that phishing is one of the leading threats in the hospitality and tourism sectors, targeting hotel bookings and customer data
- **Financial Fraud (35%):** This figure aligns with the reported impact of ATM skimming, fraudulent transactions, and fake payment systems widely discussed in industry reports and the shared document
- **Public Wi-Fi Exploitation (20%):** Data from Norton and Kaspersky highlights the prevalence of public Wi-Fi risks, with many tourists connecting to unsecured networks

- Document and Logistical Risks (15%): Incidents of fake bookings and digital document fraud have been consistently reported by IATA and Travel Pug, though they are less frequent than phishing or financial fraud

By understanding these statistics and trends, both businesses and travelers can better prepare to mitigate cybersecurity risks in the travel industry. The insights demonstrate the urgent need for adopting robust security measures to protect sensitive information and systems from evolving threats.

## **CYBER-SECURITY GUIDE FOR TOURISTS AND TRAVELERS**

In today's interconnected world, cybersecurity is a critical aspect of ensuring safe and secure travel. Tourists and customers must remain vigilant and adopt strategies to protect themselves from potential cyber threats (Fig. 7).

Here are key recommendations to enhance your cybersecurity while traveling:

### **1. Use Secure Networks**

Avoid using public Wi-Fi networks whenever possible, as they are often unsecured and can be exploited by cybercriminals. If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your data and protect your online activities.

### **2. Keep Devices Updated**

Ensure all your devices, including smartphones, tablets, and laptops, are updated with the latest software and security patches. Regular updates help address vulnerabilities and keep your devices more secure.

### **3. Strengthen Passwords and Use Two-Factor Authentication (2FA)**

Create strong, unique passwords for all your accounts, avoiding predictable combinations. Enable two-factor authentication (2FA) for an extra layer of security, especially for email, banking, and travel-related accounts.

### **4. Be Cautious with Online Transactions**

When making online bookings or purchases during your travel, ensure the website is secure. Look for the padlock icon in the browser's address bar and verify that the URL begins with "https://." Avoid entering sensitive information on suspicious websites or links.

### **5. Protect Personal Information**

Limit the sharing of personal information on social media or other platforms while traveling. Oversharing can provide cybercriminals with data they could exploit.

### **6. Backup Important Data**

Regularly back up your important data, such as travel documents, photos, and itineraries, to a secure cloud service or external storage device.

This ensures you have access to your information even in case of device loss or theft.

### **7. Beware of Phishing Attempts**



Exercise caution when opening emails or messages from unknown sources. Avoid clicking on suspicious links or downloading attachments that could contain malware.

### 8. Secure Your Devices Physically

Keep your devices in a safe location when not in use. Use biometric authentication, such as fingerprint or facial recognition, where available, to prevent unauthorized access.

### 9. Limit Bluetooth and NFC Usage

Disable Bluetooth and Near Field Communication (NFC) on your devices when not in use to reduce the risk of unauthorized access or data theft.

### 10. Invest in Reliable Security Software

Install trusted antivirus and anti-malware software on your devices to detect and neutralize potential threats.



Fig. 7. A Cyber-security guide for the traveler. *Source: Authors*

By adopting these practices, travelers can substantially reduce their exposure to cyber threats and navigate the digital landscape of modern tourism with far greater confidence. A proactive approach to cybersecurity not only protects sensitive data and financial resources but also ensures that unexpected digital disruptions do not interfere with the enjoyment and purpose of the trip. In an era where nearly every aspect of travel – from booking flights to unlocking hotel rooms – relies on technology, even small preventive actions can create a meaningful barrier between a secure journey and a compromised one.

Empowered with awareness, equipped with essential tools, and guided by responsible online behavior, travelers can transform themselves from vulnerable targets into informed digital citizens capable of recognizing, avoiding, and responding to emerging virtual risks. Ultimately, cybersecurity becomes more than a protective measure – it becomes an integral part of smart, sustainable, and stress-free travel in the digital age.

## CONCLUSION

The digital transformation of the tourism industry has undeniably enhanced the convenience, personalization, and overall efficiency of travel. Online booking platforms, mobile applications, and AI-driven services have redefined how tourists plan, navigate, and experience destinations. Yet, this rapid technological evolution has simultaneously introduced a complex ecosystem of virtual risks that threaten both individual travelers and the broader tourism sector. As demonstrated throughout this study, the rise of financial fraud, document-related scams, technical vulnerabilities, and large-scale data breaches underscores the urgent need to address cybersecurity as a core component of sustainable tourism development.

The findings reveal that cyber threats such as phishing attacks, ATM skimming, fraudulent payment systems, and the exploitation of unsecured public Wi-Fi networks remain among the most prevalent and damaging risks. The quantitative evidence presented shows a consistent upward trend in cyber incidents, with regions like Southeast Asia and Europe emerging as hotspots due to their high levels of digital adoption and heavy tourism flows. These patterns highlight that virtual risks are no longer isolated incidents but systemic challenges that require coordinated responses.

At the same time, emerging technologies – including blockchain, AI-enhanced fraud detection, biometric authentication, and secure IoT ecosystems – offer promising pathways to strengthen cybersecurity defenses in tourism. Their successful implementation, however, depends on sustained collaboration between governments, tourism businesses, cybersecurity experts, and technology providers. Without shared standards, regulatory alignment, and multi-stakeholder engagement, even the most advanced tools will struggle to achieve their full protective potential.

To meaningfully mitigate these threats, proactive measures must be embraced at both the individual and organizational levels. Travelers should adopt essential cybersecurity practices, such as using VPNs, avoiding unsecure public networks, regularly updating device software, and exercising caution when interacting with unfamiliar digital platforms.

Tourism businesses, in turn, must prioritize data protection and operational resilience through Zero Trust security models, stronger encryption standards, employee training, and the continuous monitoring of digital infrastructure. Transparency about risks and informed customer education should also become standard components of the tourism experience.

Addressing the existing barriers – such as the financial burden of cybersecurity investments, the lack of technical expertise in smaller enterprises, and the relentless evolution of cyber threats – will



require long-term strategic planning. Policy makers must support the sector through clear regulatory frameworks, funding for cybersecurity innovation, and mechanisms for international cooperation. As virtual risks transcend national borders, global partnerships and shared intelligence networks are essential for establishing a secure digital travel ecosystem.

Ultimately, fostering a culture of cybersecurity awareness is fundamental to safeguarding the integrity of the tourism industry. Protecting tourists' digital identities, financial assets, and personal data is not only a technical necessity but also a prerequisite for maintaining trust in digital tourism services. The results and recommendations outlined in this research provide a foundation for developing comprehensive strategies that balance innovation with robust security. By doing so, the tourism industry can ensure that technological advancement continues to enhance – not endanger – the travel experience, supporting a safer, more resilient, and future-ready global tourism sector.

### ***Declaration by Authors***

**Ethical Approval:** Approved

**Acknowledgement:** None

**Source of Funding:** None

**Conflict of Interest:** The authors declare no conflict of interest.

## **REFERENCES**

- Boto-García, D. (2023). Hospitality workers' awareness and training about the risks of online crime and the occurrence of cyberattacks. *Journal of Hospitality and Tourism Management*, 55, 240–247. <https://doi.org/10.1016/j.jhtm.2023.04.010>
- Boutin, C. (2021, March 3). NIST offers cybersecurity guide tailored to hospitality industry. *National Institute of Standards and Technology*. <https://www.nist.gov/news-events/news/2021/03/nist-offers-cybersecurity-guide-tailored-hospitality-industry>
- Business Wire. (2021, November 9). Cyber threats have increased 81% since global pandemic. *BusinessWire*. <https://www.businesswire.com/news/home/20211108005775/en/Cyber-Threats-Have-Increased-81-Since-Global-Pandemic>
- Centrix. (n.d.). *5 Ways to Protect Your Tourism Business from Cybersecurity Threats*. Retrieved from <https://www.centrix.com.au/5-ways-to-protect-your-tourism-business-from-cybersecurity-threats/>
- Cukier, M. (2007). *Hackers Attack Every 39 Seconds*. University of Maryland. Retrieved December 2024, from <https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds>
- Cyberint. (2025, June). *Travel & Tour Operations Industry Threat Landscape Report (Public Edition)*. Retrieved November 12, 2025, from <https://cyberint.com/wp-content/uploads/2025/06/Travel-Threat-Landscape-Report-Public-2.pdf>
- Florido-Benítez, L. (2025). The role of cybersecurity as a preventive measure in digital tourism and travel: A systematic literature review. *Discover Computing*. Advance online publication. <https://doi.org/10.1007/s10791-025-09523-3>
- Gallagher, U.S. (2022). *Phishing Attacks Targeting the Hospitality Industry: Hotel Industry Cyber Update – September 2022*. Retrieved September 2024, from <https://www.ajg.com/us/news-and-insights/2022/oct/hotel-industry-cyber-update-september-2022>



- Gwebu, K., & Barrows, C. W. (2020). Data breaches in hospitality: Is the industry different? *Journal of Hospitality and Tourism Technology*, 11(3), 511–527. <https://doi.org/10.1108/JHTT-11-2019-0138>
- IATA (International Air Transport Association). (2023). *Digital Document Fraud in Air Travel: A Growing Challenge*. Retrieved from <https://www.iata.org/en/pressroom/2023-digital-documents>
- IBM. (2023). *Phishing and Hospitality: Annual Security Report*. Retrieved December 2024, from <https://www.ibm.com/phishing-hospitality-report-2023>
- Identity Theft Resource Center. (2023). *The Financial Impact of Identity Theft*. Retrieved December 2024, from <https://www.idtheftcenter.org/financial-impact-2023>
- International Air Transport Association (IATA). (2023). *Digital Document Fraud in Air Travel: A Growing Challenge*. Retrieved December 2024, from <https://www.iata.org/en/pressroom/2023-digital-documents>
- Karadayi-Usta, S. (2024). Cybersecurity risks analysis in the hospitality industry: A stakeholder perspective on sustainable service systems. *Systems*, 12(10), 397. <https://doi.org/10.3390/systems12100397>
- Kaspersky. (2023). *Public Wi-Fi Risks for Travelers: Research Study 2023*. Retrieved December 2024, from <https://www.kaspersky.com/travel-wifi-risks>
- Kaspersky. (2017). How to avoid public Wi-Fi security risks. *Kaspersky Resource Center*. <https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks>
- Kindzule-Millere, I., & Zeverte-Rivza, S. (2022). Digital transformation in tourism: Opportunities and challenges. *Economic Science for Rural Development*, 56, 476–486. <https://doi.org/10.22616/ESRD.2022.56.047>
- Nam, K., Dutt, C. S., Chathoth, P., & Khan, M. S. (2021). Blockchain technology for smart city and smart tourism: Latest trends and challenges. *Asia Pacific Journal of Tourism Research*, 26(4), 454–468. <https://doi.org/10.1080/10941665.2019.1585376>
- Norton. (2023). *Consumer Cyber Safety Report: Risks for Tourists in 2023*. Retrieved December 2024, from <https://us.norton.com/cyber-safety-tourism-2023>
- Porter, L. (2024, March 12). Cyber security threats in tourism and hospitality: How to keep guests safe. Training Camp. Retrieved November 12, 2025, from <https://trainingcamp.com/articles/cyber-security-threats-in-tourism-and-hospitality/>
- Rashideh, W. (2020). Blockchain technology framework: Current and future perspectives for the tourism industry. *Tourism Management*, 80, 104125. <https://doi.org/10.1016/j.tourman.2020.104125>
- Statista. (2022). *Phishing Emails Across Industries: Phishing Continues to Pose Major Risk Despite a Decrease in Cyberattacks*. Retrieved December 2024, from [https://www.statista.com/press/p/technology\\_market\\_insights\\_cybersecurity\\_2022/](https://www.statista.com/press/p/technology_market_insights_cybersecurity_2022/)
- Statista. (2023). *Phishing Scams in Tourism: Annual Report*. Retrieved December 2024, from <https://www.statista.com/reports/2023-phishing-tourism>
- Symantec. (2022). *The State of Phishing Attacks in Hospitality: Cybersecurity Insights*. Retrieved December 2024, from <https://www.symantec.com/hospitality-phishing-attacks>
- Tourism Tribe. (n.d.). *Protect Your Tourism Business from Cyber Security Threats*. Retrieved from <https://www.tourismtribe.com/protect-your-tourism-business-from-cyber-security-threats/>
- Travel Pug. (2024a). *Public Wi-Fi Exploitation: 20 Common Tourist Scams in Southeast Asia (And How to Avoid Them)*. Retrieved October 2024, from <https://travelpug.net/20-common-tourist-scams-in-southeast-asia-and-how-to-avoid-them/>



- Travel Pug. (2024b). *Fake Booking Platforms: 20 Common Tourist Scams in Southeast Asia (And How to Avoid Them)*. Retrieved December 2024, from <https://travelpug.net/20-common-tourist-scams-in-southeast-asia-and-how-to-avoid-them/>
- The Daily Telegraph. (2024). *Digital Document Fraud: Common Scams That Are Catching Out Aussie Travellers*. Retrieved December 2024, from <https://www.dailytelegraph.com.au/lifestyle/the-great-escape-travel-survey-common-scams-that-are-catching-out-aussie-travellers-and-how-to-avoid-them/news-story/f36e3e2ecc3a9e52e992b208662414d>
- ReportLinker. (n.d.). *Cybercrime and Cybersecurity Market Trends*. Retrieved from <https://www.reportlinker.com/market-report/Cybersecurity/517797/Cybercrime?term=cyber%20threat%20trends>
- UpGuard. (n.d.). *Cybersecurity in the Hospitality Industry*. Retrieved from <https://www.upguard.com/blog/cybersecurity-in-the-hospitality-industry>
- UpGuard. (n.d.). *Reduce Cybersecurity Risk*. Retrieved from <https://www.upguard.com/blog/reduce-cybersecurity-risk>
- VISA Agency, Bali. (2023). *ATM Skimming in Southeast Asia: How to Avoid Card Skimming in Bali*. Retrieved December 2024, from <https://balivisasagency.com/how-to-avoid-card-skimming-in-bali/>
- Yallop, A. C., Gică, O. A., Moisescu, O. I., Coroş, M. M., & Séraphin, H. (2023). The digital traveller: Implications for data ethics and data governance in tourism and hospitality. *Journal of Consumer Marketing*, 40(2), 155–170. <https://doi.org/10.1108/JCM-12-2020-4278>

#### **How to cite this article:**

Karadzhev, V. & Yuleva-Chuchulayna, R. (2025). Virtual Security Risks During Tourist Travel. A Cyber-Security Guide for Travelers. *International Journal of Digital Research*, E-ISSN: 3033-179X, Vol. 1(4): 23-43. <https://doi.org/10.63711/ijdr.net20250402>

\*\*\*\*\*

