Journal of Association of Arab Universities for Tourism and Hospitality (JAAUTH)

journal homepage: http://jaauth.journals.ekb.eg/

Exploring the Role of Cybersecurity in Enhancing Digital Trust of Egyptian Travel Agencies

Reham Mamdouh Abd El-Maksoud

Tourism Studies Department- Faculty of Tourism and Hotels-Mansoura University-Egypt

ARTICLE INFO

Keywords:

Cybersecurity;
Cyber hygiene;
Digital Trust;
Travel Agencies.

(JAAUTH) Vol.26, No.1, (2024), pp.185 -204.

Abstract

The travel and tourism sector 's cyber ecosystems have been highly exposed to security risks, as this sector is being highly digitalized adopting emerging technologies. Despite a lot of evidence indicating the increasing vulnerability of travel and tourism systems to cybersecurity threats, there is still limited literature applied on the tourism sector. Hence, this research aims at enhancing awareness of the application of cybersecurity and the related term of cyber hygiene, as well clarifying the importance of cybersecurity in tourism and its role in reinforcing digital trust of travel agencies. A survey was designed and distributed to a random sample of relevant managers and employees in Egyptian travel agencies to identify the extent of interest of cybersecurity in Egyptian travel agencies and its role in enhancing digital trust, 403 valid responses were analyzed by using SPSS Version. 28. The findings of this research proved that travel agencies which have an interest in cybersecurity can strengthen the digital trust of their customers. The research recommended the need for travel agencies to educate employees in cybersecurity, the necessity of having a department specialized in cybersecurity, and taking the necessary procedures to secure tourism networks, due to the effective role of cybersecurity in achieving digital trust.

Introduction

Nowadays, Markets are becoming a cyberspace, therefore they are facing a new challenge to protect people against cyber threats (e.g., internet frauds and identity thefts) (Maguilo, 2016) Cyberspace signifies a complex of all communication networks, databases, and sources of information (Cavelty, 2015). As the Egyptian vision includes advancing its infrastructure in accordance with the international standards by integrating technological systems in managing and linking infrastructure components, which results in increasing cyber-attacks that may lead to the disruption of these services (Abdel-al et al., 2022).

Today cyber risk draws more attention, particularly for fields that deal with sensitive data like tourism businesses. That issue put emphasis on managing cyber insecurity and digital privacy to protect from losses (Arcuri et al., 2020). Cyberattacks lead to critical financial,

legal, and regulatory losses that could negatively affect customer trust and brand reputation. As well, nearly more than $500,000 were costed to recover from a security hack in more than 5500 companies from different fields in 26 countries around the world (Kaspersky, 2018). For example, in 2018 British Airways received a fine of $230 million for failure of protecting passenger data in a 2018 data hack (Olson, 2019). Cybersecurity Ventures (2020) expected that global cybercrime's costs will increase 15% per year between the years of 2021 and 2025, and reach 10.5 trillion USD by 2025, comparing to 3 trillion USD in 2015. The growing digital footprint of travel and tourism sector in the fourth industrial revolution results increasingly exposed to cyber threats either through online transactions, customer analytics, cloud integration, connected devices, or digital payment technology (Paraskevas, 2022). As in 2022 the travel and leisure sector exposed to increasing cyberattacks globally by 60% in comparison with 2021 (Desku, 2002). Hence there is an urgent need for companies to invest in cybersecurity infrastructures to protect their system networks against breached access and data modification. That in return will reduce cyber-attacks that can negatively influence companies' activity, as well as trust in online transactions and client interactions (Vasiu and Vasiu, 2018).

The findings of this study could be beneficial for tourism entities in defending the risk of business information security in tourism, raising awareness about the importance of cybersecurity, particularly in tourist countries like Egypt and could be also useful for enhancing digital trust of travel agencies.

According to Paraskevas (2022), There is a need for increasing knowledge of the implementation of cybersecurity in travel and tourism. Hence, the research problem can be formulated in two questions:

-Is there an interest of cybersecurity in Egyptian travel agencies?

- Is there an impact of cybersecurity on enhancing digital trust of travel agencies?

There is limited research that discusses concepts of cybersecurity and related terms as cyber hygiene and their role in the tourism sector. Thus, this paper aims to a. clarify concept of cybersecurity and related term of cyber hygiene, b. differentiate between concepts of cybersecurity and cyber hygiene, c. highlight the importance of cybersecurity in tourism industry, d. clarify the concept of digital trust and its importance, and e. examine the role of cybersecurity in enhancing digital trust for travel agencies.

1. Literature Review

1.1. The Concept of Cybersecurity and related term of Cyber Hygiene

Although the emergence of the term Cybersecurity many years ago, but it has gained popularity after the usage of the term by the United States President Barack Obama in 2009 (Schatz et al., 2017). With the rising number of devices connected to the internet, internet of things " IoT ", cybersecurity becomes crucial for all businesses. Cybersecurity is also known as computer security or information technology security (Khari et al., 2017), however cybersecurity is more comprehensive (Tawfiq and Mousa, 2023) as it is defined as protecting data, networks, programs, and computers in cyberspace from unauthorized access or damage or theft (Khari et al., 2017) through both technical and non-technical activities and measures meant to secure the bioelectrical environment and its included data (Cavelty, 2015). A company or organization should first and foremost pay attention to a cybersecurity, as a company relied on cybersecurity can realize high successes because of its ability to secure private and customer data against rivals (Rodríguez-deArriba et al., 2021). It becomes

popular in companies to have a security unit which is responsible for cybersecurity related standards and solutions (Li & Liu, 2021).

There is also another concept that is very important to clarify and differentiate from cybersecurity. This concept is cyber hygiene; it is considered as a good model for reducing the cost of cybersecurity, as it works to enhance its value without the need for exorbitant costs, as it works to reduce hacking of systems and networks by following the best of its practices (Ebrahim et al., 2022). Cyber hygiene is defined as the practices of cybersecurity that online customers should engage in the protection of their personal information on their internet enabled devices from being cyber attacked (Vishwanath et al., 2020). Some of these practices could be such as regularly erasing cookies, usage of credit cards instead of debit cards, data backing up, using secure browsers, and updating virus protection programs (Singh et al., 2020). Cyber hygiene is often compared to personal hygiene. As individuals practice personal hygiene to keep a good state of health, similarly digital hygiene practices can keep information and data well secured, which protects devices from external attacks and makes them function properly (Brook, 2018). Cyber security differs from cyber hygiene or also as known digital hygiene, but they are related to each other. As, cyber-hygiene is in charge of an individual while cyber-security is in charge of an institution or a group that is related to professional activities (Singh et al., 2020).

1.2 Cybersecurity in Tourism Industry

Cybersecurity is a new challenge that confronts tourism entities. Despite the importance of cybersecurity, there is still limited literature applied on the tourism sector (Kovačić et al., 2022). Cybersecurity depends on four main elements as following:

a. The 'Awareness Index' that refers to the awareness related to cyber information (e.g. if the firm systemically registers anomalies or if it realizes the suppliers ' security policies);

b. The 'Defense Index' that implies the capability of firms to defend themself from cyber violations (limiting usage of personal e-mails, prohibiting usage of personal electronic devices);

c. The 'Policy Index' that refers to the application of security-related policies as usage of operator security plans;

d. The 'External Independence Index' that includes the connectivity of internal systems and external service providers (Maguilo, 2016).

There are many reasons for cyber risks in the travel and tourism sector, this sector is increasingly exposed to cybercrimes because of its large fragmentation, complexity of the travel booking and payment networks because of the huge number of agents and third-party service providers, and the weak defenses of its legacy IT and point-of-sale systems (Paraskevas, 2022). Cybercriminals seek for financial gain from the wealth of data at travel and tourism networks that called as dark web, as these cybercriminals use stolen credit cards or reward points from hacked traveller accounts to buy travel services which they can offer at a discount of their retail value to others (Bridge, 2017). Sending emails has always been the most popular pattern of cyberattack; targeted travel institutions often receive emails involving links asking them to log in to their accounts or to repair a technical problem by searching on employees' preferences and interests to persuade them that the email originates from a legitimate source in order to download attachments with malware or provide access data. As in 2017, many travel agencies received emails that seemed to come from Sabre involving links requesting to verify their login credentials. Once travel agents logged in, the cybercriminals captured their credentials and then used them to make deceptive bookings

(Biesiada, 2017). As well, "Carbanak/Anunak attack" was considered the most popular malware attack in tourism sector, the cybercriminals asked to send their information to the agent via email through a call because of their inability for using reservation system. The sending email attachment to tourism offices contained malware capable of stealing local passwords, searching user's email, targeting payment systems, or installing completely different remote desktop programs and targeting credit card data by scraping memory on point-of-sale systems (Trustwave, 2016).

As a result of the increased number of cybercrimes, there is an urgent need for protection of business systems in tourism institutions (DeFranco and Morosan, 2017; Ruzic and Matika, 2020). Holdsworth and Apeh (2017) found that reasons for cyber risks in tourism are due to inexperienced employees and low awareness of the importance of cybersecurity. Many experts found that the main reason for information security violations is due to employees' behavioural factors rather than technical issues per se, as employees are a key data security factor (Dhillon & Backhouse, 2000). As well, high employee turnover in the travel and tourism is considered another reason for vulnerability of security protocols (Paraskevas, 2022). Employees can be the origination point for information violations through inadvertent leakage of information via removable devices or internet connections (Choi et al, 2018). The tourism sector suffers from cyber threats that can be handled through a new and better organisation policy depending on highly awareness of all stakeholders (Maguilo, 2016).

Many studies have drawn attention to measuring the level of application of cybersecurity in organisations in various fields, as Alghamdi & Almostadi (2021) have measured the level of cybersecurity in terms of confidentiality, privacy, and reinforcement. Cybersecurity is also measured according to dimensions of regulatory framework, company procedures, systems preparedness, cyber training and awareness, individuals, and compliance monitoring (Kanwal et al., 2022). While cybersecurity includes three critical elements namely confidentiality, integrity, and availability (Borky & Bradley, 2019; Al-Manea, 2022). This study depends on measuring the level of cybersecurity in travel agencies according to three dimensions, namely confidentiality, privacy, and reinforcement (Alghamdi & Almostadi, 2021). Confidentiality refers to maintenance of information by granting permission to only those authorized to access that information and data, while preventing unauthorized persons from accessing that information (Al-Manea, 2022). The second dimension 'privacy' indicates to the capability of firms to control over information about them, as well controlling over who can observe them (Van Bogaert& Ogunbanjo, 2009). The third dimension 'reinforcement' is defined as means of development, raising efficiency, and improving skills for protecting a firm against cyber-attacks (Alghamdi & Almostadi, 2021).

In the context of tourism and hospitality concerning cybersecurity, Maguilo (2016) has found the significance of cybersecurity for enhancing competitiveness of Italian tourism destinations. While Chen & Fiscus (2018) have reviewed information security attacks of the hospitality industry in USA and thus concluded the importance of cybersecurity and the need of cyber-attacks analysis in the hospitality sector. Bazazo et al., (2019) has found the significance of cybersecurity for mainly protecting digital bases in all important tourist facilities. Also, Arcuri et al. (2020) concluded that cyberattacks negatively affect the economic value of hospitality companies. While Ruzic & Matika (2020) have concluded the impacts of cybercrime security threats on Croatian business institutions in tourism. Also, Alghamdi & Almostadi (2021) have revealed the significance of cybersecurity in achieving competitiveness in the field of aviation services. While Kovačić et al., (2022) have revealed through the conducted bibliometric analysis in the context of tourist destinations and tourism

in general, that there is insufficient number of studies research the mechanisms of increasing cybersecurity in tourism.

This paper is a continuation of previous studies, aiming to increase awareness about cybersecurity and examine the relationship between cybersecurity and digital trust in the tourism industry.

1.3 Concept of Digital Trust and its Importance

In the era of digital transformation, it becomes crucial to create consumer digital trust. As, the level of trust of online transactions is less than in traditional ones because of uncertainty concerning the behaviour of e-vendors or the perceived risk of cybercriminals (McKnight et al., 2002; Grabner- Kräuter and Kaluscha, 2008). Pietrzak and Takala (2021) describe digital trust as the measure of confidence that employees, clients, partners, and other stakeholders have in a company's capability to secure data and privacy of individuals. Also, Marcial and Launer (2019) and Launer et al. (2022) referred to digital trust as the general belief that technology, people, and processes are aligned in ways that will meet individuals' digital expectations, like sense of confidence, security, or control to enhance providing a secure digital environment. The confidence of clients in the safety and dependability of digital systems and services either for example in online financial transactions or the privacy of their personal information mainly depends on digital trust. Building and maintaining trust in the digital field is an ongoing challenge that requires firmly safeguarding of sensitive information and successfully resisting the attacks of malicious activities (Chui, 2023).

Considering the dependent variable of digital trust in the context of tourism and hospitality, Öztüren (2013) has referred to the impact of electronic trust through online travel social networks on tourism industry by sustaining the relationships with their clients. While Launer & Cetin (2021) have measured the level of digital trust of employees in the workplace by applying on institutions in the hotel industry and have concluded that the wholesale companies in the hotel supply chain have greater digital trust levels considering pillars of technology, people and digital process, in comparison with all the other companies (particularly compared with the hotel or restaurant and farming agriculture companies).

Chui (2023) referred to the highly significance of digital trust and it can be measured through four pillars of security, dependability, integrity, and authenticity. While Launer & Cetin (2021) and Launer et al. (2022) measured the degree of digital trust in terms of the technology used, people involved, and the digitalization process. Öztüren (2013) concluded that dimensions of e-trust include ability or competence, integrity, benevolence, and predictability. This study depends on measuring digital trust including three essential dimensions, namely the technology used, people involved, and the digitalization process (Launer & Cetin, 2021; Launer et al., 2022)

People are considered the most essential element for the effective operation of all information systems, Thus, individuals who manage processes, programs, and maintain an information system play a critical role in building digital trust. While the dimension of used technology refers to hardware, software, databases, and telecommunications. The third dimension of digital process refers to elements that collect, operate, store, disseminate, and secure data (Launer & Cetin, 2021).

1.4.Role of Cybersecurity in Enhancing Digital Trust

As being in the era of electronic commerce, decreasing digital trust had been considered among the critical challenges in online shopping and payment transactions. Concerns of the security, many clients avoid purchasing of travel products online, thus businesses should care

about constructing a strong trust and providing a highly secure environment to raise businesses 's customers trust and sustain the relationships with their clients (Tan and Thoen, 2001; Chen, 2006; Bauernfeind and Zins, 2006; Hsu & Kang, 2013).

With the increasing reliance on digital infrastructure, technology is still vulnerable, as the confidentiality and safety of the information and communication technology infrastructure is exposed to cyber threats, which leads to decrease trust in the use of information and communication technology because of the lack of cybersecurity (Farag, 2022). Hacking of information security has negative impacts including losses of stakeholder trust, deterioration of reputation and damage to the brand as well as decreasing future profits (Gordon, et al., 2003). As El-Bishi (2021) concluded that because of the huge amount of data, digital transformation and highly dependence on technical systems resulting to the urgent need of building a culture to protect information and systems, so that systems and networks are protected and users' trust in these networks and information will be increased, as their data are protected and can be used at the appropriate time. Hence the negative consequences of breaches put an emphasis on the importance of cybersecurity, as breaches of systems can lead to for example, negative word-of-mouth and decreased customer satisfaction (Berezina et al., 2012). Accordingly, it becomes crucial increasing employees' awareness of information security through protocols for training employees to be conscious of what information is permitted to be provided to the public and identify suspicious activities in order to handle data properly and decrease breaches (Chen& Fiscus, 2018).

Many efforts were made by Egypt to enhance confidence in the communication and information infrastructure, its applications, and services in various sectors in order to achieve a safe and reliable digital environment. Among these efforts the establishment of Egyptian Computer Emergency Readiness Team (EGCERT) since 2009 to confront cyber security threats and the issuance of the National Cyber Security Strategy (2022-2026) (Abdel-al et al., 2022). According to the growth of smart tourism and expansion of digitalization in all aspects of the tourism sector as electronic booking systems and others in the tourism sector (Burns& Roberts, 2013; Khwaldeh et al., 2017; Bazazo et al ., 2019) that put emphasis on the importance of applying better requirements, standards and safe practices to decrease breaches of tourist databases and protect these digital databases through creating a number of controls on the basis of confidentiality and integrity of information in tourist databases (Bazazo et al ., 2019) .

2.Research Methodology

2.1. Data Collection and Sample Size

The researcher has used an online questionnaire for gathering data for this study, as internet-based data collection methods have acquired lately popularity particularly in quantitative research methodology (Van Selm and Jankowski, 2006). The survey was tested to assure its clarity, by distributing it to two experts in the field of tourism and information technology to avoid uncertain phrasing or terminology, as well distributing it to some members of academic professors and was modified due to their observations. And then directed to the investigated sample of relevant directors and employees in travel agencies (Class A) operating in Arab Republic of Egypt which are estimated 2220 travel agency according to statistics of ETAA (2023) during the period from July 2023 to September 2023. Detecting the size of the investigated sample depends on random sample size as it was the optimal method to be adopted to this research for the difficulty to determine the size of the population study of employees of Egyptian travel agencies.

Participants received a questionnaire through the e-mail addresses of Egyptian travel agencies, as well sending an invitation message through social media platforms either Facebook or WhatsApp requesting to fill out the survey via google form which is in Arabic language and asking them to forward the invitation to their colleagues who also work in investigated travel agencies 'snowball sampling'. Valid 403 responses were received and analyzed by using SPSS V.28.

2.2. Research Instrument

The questionnaire form consists of (41) questions divided into three sections. Section one relates to profile data that consists of (7) questions about (tourism company name (optional question), employee gender, age, work experience in the field of tourism and tourism companies in general, administrative level, inquiring about existence of department for information security and cybersecurity in tourism company, number of training courses in cybersecurity). The second section relates to assessing the interest of cybersecurity in tourism companies according to three dimensions of confidentiality, privacy, and reinforcement including (18) questions, While the last section relates to the impact of applying cybersecurity on the digital trust of travel agencies according to three dimensions of technology used (digital systems), users' experience, and processes consisting of (16) questions. The study was based on using 5-points Likert scale (ranged from strongly agree =5 to strongly disagree =1).

2.3.Data Analysis Measures

The results include three main phases. Descriptive analysis was utilized to examine participants' responses; mean was used to describe the opinions of the study sample about the study variables, standard deviation was used to measure the amount of variability or dispersion around an average (mean), frequencies and percentage were used to represent statistics for comparing values, T- test was conducted for determining a significant difference in the mean of the study population from which the sample was extracted from a fixed value, and regression and correlation were used to examine the relationship between variables.

2.4.Reliability and Validity:

As indicated in the following Table (1), the questionnaire's reliability and validity of this study were measured depending upon Cronbach's Alpha coefficient.

Table 1. Reliability Coefficient

Axes of the study	No of items	Cronbach's Alpha
1. Assessing the interest of cybersecurity in travel agencies.	18	0.914
2. Impact of applying cybersecurity on the digital trust of travel agencies.	16	0.865
Total	34	0.928

As shown from the previous table, research instrument is characterized by a high reliability coefficient (0.928), as values of reliability coefficient ranged from 0.865 to 0.914, indicating the capability of the instrument in general to realise the aims of the study. As according to Sekaran & Bougie (2016) indicated that values which are convenient for implementation of the questionnaire to the study (Alpha≥ 0.60).

3.Results and discussion

3. 1. Profile Data of Study Sample

Table 2. Demographic Data of the study sample

Demographic Data	Attribute	Statistics		Rank
		Freq.	%	
Gender	Male	211	52.4	**1**
	Female	192	47.6	**2**
Total		**403**	**100%**	
Age	Less than 30 years	102	25.3	**2**
	From 30 – less than 40 years	80	19.9	**٣**
	From 40 -Less than 50 years	181	44.9	**١**
	50 years and over	40	9.9	**4**
Total		**4.3**	**100%**	
Work experience	Less than 5 years	102	25.3	**2**
	From 5 to less than 10 years	80	19.9	**4**
	From 10 to less than 15 years	90	22.3	**3**
	15 years and over	131	32.5	**1**
Total		**4.3**	**100%**	
Administrative level	Senior Management	181	44.9	**1**
	Middle Management	51	12.7	**3**
	Direct Management (Staff)	171	42.4	**2**
Total		**403**	**100%**	
Work department	Management	171	42.4	**١**
	Information Technology	20	٥.5	**٥**
	Ticketing	131	32.5	**٢**
	Marketing	51	12.7	**٣**
	Sales	30	7.4	**٤**
Total		**4.3**	**100%**	

As shown in table 2, the study sample successfully captured a fairly even representation of **gender**, with (52.4%) of respondents reporting female and (47.6%) reporting male. According to the **age group** of the study sample, the largest proportion of the sample (44.9%) was between 40-50 years, then (25.3%) of less than 30 years, followed respectively by the age group ranged from 30-40 years, then older than fifty, with percentages of (19.9% and 9.9%) respectively. That indicates the diversity of age groups of the investigated sample. While the study sample distribution regarding **work experience** was more than 15 years at the first rank indicating the long experience of participants in the field of tourism companies' business resulting to their respondents can provide valuable views as they have adequate experience. The largest proportion of the sample due to **administrative level** was at senior management (44.9%), This is because most of the study sample was from executives, as they are the best to deal with paragraphs of the survey. As well the investigators belong to different departments; management (42.4%), ticketing (32.5%), marketing (12.7%), sales (7.4%), and information technology (5.5%). This refers to the variety of administrative departments to which the participants belong, resulting in diversity of functional backgrounds of study sample.

Table 3.

Existence of department for information security and cybersecurity in travel agencies

Factor	Variables	Frequency	Percentage (%)	Rank
Is there a department for information security and cybersecurity in your travel agency?	Yes	141	35.0	**2**
	I don't know	20	5.0	**3**
	No	242	60.0	**1**
Total		403	**100%**	

As shown in table 3, high proportion of respondents at 60% refers to non-existence of a department for information security and cybersecurity in their travel agencies, followed by 35% of sample has referred to existence of the department, while 5% of sample referred to unknowing of existence of the department. That illustrates a lower percentage of the investigated participants belong to the information technology department at 5.5% from investigated sample due to non-existence of this department in a high proportion of travel agencies. This refers that there is not enough attention to information security and cybersecurity in travel agencies in Egypt, despite its great importance. This is agreed with the findings of the study of Li & Liu (2021) that refers to the need for companies to have a security unit which is responsible for cybersecurity related standards and solutions.

Table 4. Number of training courses in cybersecurity

Factor	Variables	Frequency	Percentage (%)	Rank
Number of Training courses in cybersecurity?	None	352	87.3	**1**
	One	31	7.7	**2**
	Two	20	5.0	**3**
	Three	0	0	**4**
	More than three	0	0	**5**
Total		403	**100%**	

It is clear from table 4 that high proportion of investigators at 87.3% referred that they had not attended training courses in cybersecurity, while low proportion referred that they had attended number of training courses ranged from one and two at 7.7% and 5% respectively. This refers to the fact that there is not enough attention to training employees in cybersecurity in travel agencies. That put emphasis on the need for training employees through protocols for training employees by sustainable courses to develop their understanding and skills. That is consistent with the study of Holdsworth and Apeh (2017), which refers to that reasons of cyber risks in tourism are due to inexperienced employees and low awareness of the importance of cybersecurity. As well as the study of Bazazo et al (2019), which indicates that there is a need for increasing awareness of the implementation of cybersecurity in tourism and hospitality. It is also consistent with the study of Kovačić et al (2022), that reveals the need for paying attention to the education of hotel staff in cybersecurity.

3.2. Assessing the interest of cybersecurity in travel agencies

Table 5. Interest of cybersecurity evidence from investigators from travel agencies

Statement	N %	5-Point Likert – Scale					Statistics		
		5	4	3	2	1	$\bar{x}$	SD	R
a- confidentiality									
1-The employee has a strong password consisting of small and large symbols, letters, and numbers.	N	51	190	140	20	2	**3.67**	**0.779**	2
	%	12.1	45.8	33.3	4.8	0.5			
2-Confidential passwords for electronic systems never exchanged between employees.	N	22	61	150	120	50	**2.72**	**1.042**	5
	%	5.2	14.5	35.7	28.6	11.9			
3-The system determines the identity of employees when accessing or modifying data.	N	63	220	100	20	0	**3.81**	**0.754**	1
	%	15.6	54.6	24.8	5				
4-The system doesn't allow the same electronic documents to be entered more than once.	N	51	181	140	20	11	**3.60**	**0.871**	3
	%	12.7	44.9	34.7	5	2.7			
5-There are strict administrative instructions about protecting the system from any fraud.	N	22	33	153	128	67	**2.54**	**1.037**	6
	%	5.2	7.9	36.4	30.5	16.0			
6-I know the system penalties for publishing and disclosing confidential documents and information.	N	32	71	140	110	50	**2.81**	**1.109**	4
	%	7.6	16.9	33.3	26.2	11.9			
Average of confidentiality dimension							**3.19**	**0.594**	1
b- Privacy									
7-All departments with the assistance of IT department review user authorities regularly.	N	20	63	150	120	50	**2.71**	**1.033**	6
	%	0.5	15.6	37.2	29.8	12.4			
8-Departments use several technologies such as: authentication, authorization, and encryption to protect sensitive systems and data.	N	41	161	150	40	11	**3.45**	**0.903**	2
	%	10.2	40.0	37.2	9.9	2.7			
9-The firewall is constantly running and updated to prevent hackers from accessing personal or company data.	N	9	150	150	58	36	**3.09**	**0.978**	4
	%	2.1	35.7	35.7	13.8	8.6			
10-Employees in your company are aware of the risks of sending personal information via text message or email.	N	33	200	80	80	10	**3.41**	**0.977**	3
	%	8.2	49.6	19.9	19.9	2.5			
11-Sensitive information of your company never be shared via social media.	N	51	181	140	20	11	**3.60**	**0.871**	1
	%	12.7	44.9	34.7	5	2.7			
12-The company directs their beneficiaries of its systems towards ways to protect and secure information.	N	32	61	140	120	50	**2.76**	**1.100**	5
	%	7.9	15.1	34.7	29.8	12.4			
Average of privacy dimension							**3.17**	**0.633**	2

c- Reinforcement									
13- Employees are monitored to ensure the application of policies and procedures to secure information	**N**	22	61	150	120	50	**2.71**	**1.042**	4
	%	5.5	15.1	2	29.8	12.4			
14- Antivirus software is regularly used in the company's devices to protect them from malware.	**N**	33	200	80	80	10	**3.41**	**0.977**	1
	%	8.2	49.6	19.9	19.9	2.5			
15- Anti-spyware software is regularly used on company devices to protect them from malware.	**N**	22	171	120	50	40	**3.21**	**1.059**	2
	%	5.5	42.4	29.8	12.4	9.9			
16-There are available Back-up periodically either on hard disks or a private cloud at the company.	**N**	2	159	139	67	36	**3.06**	**0.968**	3
	%	0.5	39.5	34.5	16.6	8.9			
17-The company publishes periodically instructions to its clients to confront cybercrimes.	**N**	2	81	150	120	50	**2.67**	**0.951**	5
	%	0.5	20.1	37.2	29.8	12.4			
18- The company provides appropriate training programs in the field of cybersecurity.	**N**	1	21	181	130	70	**2.39**	**0.840**	6
	%	0.2	5.2	44.9	32.3	17.4			
Average of reinforcement dimension							**2.91**	**0.741**	3
Average of all Responses							**3.٠١**	**0.٦١٥**	

As shown in Table 5, results from respondents referred that level of interest of cybersecurity in travel agencies is to some extent, as high proportion of responses were towards neutral (AV Mean= 3.01, SD= 0.615). That leads to cyber risks in the travel and tourism sector, as this industry is increasingly vulnerable to cybercrimes due to its large fragmentation, complexity of the travel booking and payment networks because of the huge number of agents and third-party service providers, and the weak defenses of its legacy IT and point-of-sale systems (Paraskevas, 2022). This study depends on measuring the level of cybersecurity in companies due to dimensions of confidentiality, privacy, and reinforcement based on the scale of Alghamdi & Almostadi (2021). The average of confidentiality comes at first rank (AV Mean= 3.19, SD= 0.594), followed by privacy (AV Mean= 3.17, SD= 0.633), and reinforcement (AV Mean= 2.91, SD= 0.741). Regarding dimension of **confidentiality**, there is an agreement for statements of (The system determines the identity of employees when accessing or modifying data, The employee has a strong password consisting of small and large symbols, letters, and numbers, and The system doesn't allow the same electronic documents to be entered more than once) at (Mean= 3.81, SD= 0.754), (Mean= 3.67, SD= 0.779), and (Mean= 3.60, SD= 0.871) respectively. While the respondents for statements of (I know the system penalties for publishing and disclosing confidential documents and information, Confidential passwords for electronic systems never exchanged between employees, and There are strict administrative instructions about protecting the system from any fraud) were towards neutral at (Mean= 2.81, SD= 1.109), (Mean= 2.72, SD= 1.042), and (Mean= 2.54, SD= 1.037) respectively.

Regarding dimension of **privacy**, there is an agreement for statements of (Sensitive information of your company never be shared via social media, Departments use several technologies such as: authentication, authorization, and encryption to protect sensitive systems and data, and Employees in your company are aware of the risks of sending personal information via text message or email) at (Mean= 3.60, SD= 0.871), (Mean= 3.45, SD= 0.903), and (Mean= 3.41, SD= 0.977) respectively. While the respondents for

statements of (The firewall is constantly running and updated to prevent hackers from accessing personal or company data, The company directs their beneficiaries of its systems towards ways to protect and secure information, and All departments with the assistance of IT department review user authorities regularly) were towards neutral at (Mean= 3.09, SD= 0.978), (Mean= 2.76, SD= 1.100), and (Mean= 2.71, SD= 1.033) respectively.

Regarding dimension of **reinforcement**, there is an agreement for statement of (Antivirus software is regularly used in the company's devices to protect them from malware) at (Mean= 3.41, SD= 0.977). While the respondents for statements of (Anti-spyware software is regularly used on company devices to protect them from malware, There are available Back-up periodically either on hard disks or a private cloud at the company, Employees are monitored to ensure the application of policies and procedures to secure information, and The company publishes periodically instructions to its clients to confront cybercrimes) were towards neutral at (Mean= 3.21, SD= 1.059), (Mean= 3.06, SD= 0.968), (Mean= 2.71, SD= 1.033) and (Mean= 2.67, SD= 0.951) respectively. There is disagreement of a statement of the company provides appropriate training programs in the field of cybersecurity at (Mean= 2.39, SD= 0.840), this result assures the result providing in table 4 of low number of training courses in cybersecurity that employees had attended.

3.3. Impact of interesting of cybersecurity on travel agencies 'digital trust

Table 6. Impact of cybersecurity on digital trust

Statement	N %	5-Point Likert – Scale					Statistics		
		5	4	3	2	1	x̄	SD	R
a- Technology used (digital systems)									
1- Information security programs enhance confidence in the system.	**N**	243	140	20	0	0	**4.55**	**0.589**	1
	%	6.3	34.7	5.0					
2- The system requires users to change passwords periodically.	**N**	181	212	10	0	0	**4.42**	**0.543**	2
	%	44.9	52.6	2.5					
3- The company has policies and plans to enhance user confidence in its systems and programs.	**N**	153	190	60	0	0	**4.23**	**0.690**	4
	%	38.0	47.1	14.9					
4- The technology used makes the digital system secure.	**N**	232	111	50	10	0	**4.40**	**0.799**	3
	%	57.6	27.5	12.4	2.5				
5- Satisfaction of the overall performance of electronic services.	**N**	153	190	60	0	0	**4.23**	**0.690**	4
	%	38.0	47.1	14.9					
Average of digital systems dimension							**4.37**	**0.418**	٢
b- Users' experience									
6- The company's reliance on experts in cybersecurity application enhances its confidence.	**N**	243	140	20	0	0	**4.55**	**0.589**	2
	%	60.3	34.7	5.0					
7- The company ensures that its employees can use various technological techniques.	N	253	90	50	10	0	**4.45**	**0.804**	3
	%	62.8	27.3	12.4	2.5				
8-There is no sharing of customers' personal data with others without obtaining the approval of their owners.	N	343	60	0	0	0	**4.85**	**0.356**	1
	%	85.1	14.9						
9- The user trusts that he can recover his data in a timely manner.	**N**	163	190	30	20	0	**4.23**	**0.791**	5
	%	40.4	47.1	7.4	5.0				
10- The company's website meets all customers' needs with confidentiality and privacy.	**N**	212	131	60	0	0	**4.38**	**0.731**	4
	%	52.6	32.5	14.9					

11- The website requests an evaluation of the provided services for continuous development of these services .	N %	153 38.0	190 47.1	60 14.9	0	0	**4.23**	**0.690**	5
Average of users' experience dimension							**4.45**	**0.358**	١
c- Processes									
12-Information security programs limit the access of viruses to company devices.	N %	223 55.3	130 32.3	40 9.9	10 2.5	0	**4.40**	**0.768**	**2**
13-Information security software protects users' data from damage.	N %	262 65	101 25.1	40 9.9	0	0	**4.55**	**0.669**	**1**
14- The electronic payment process on the website is well secured.	N %	153 38.0	120 29.8	90 22.3	40 9.9	0	**3.96**	**1.000**	**3**
15-Information security programs reduce frequent email breaches.	N %	153 38.0	120 29.8	90 22.3	40 9.9	0	**3.96**	**1.000**	**3**
16-The company applies security standards to enhance protecting users' data.	N %	153 38.0	120 29.8	90 22.3	40 9.9	0	**3.96**	**1.000**	**3**
Average of processes dimension							**4.17**	**0.719**	٣
Average of all Responses							**4.32**	**0.441**	

As indicated in Table 6, the data state that there is a strongly agreement that cybersecurity has a positive impact on reinforcing digital trust of travel agencies (AV Mean= 4.32, SD= 0.441). This result is agreed with the study of El-Bishi (2021), which found that cybersecurity enhances digital trust applying it on Saudi universities. It is also agreed with the study of Farrag (2022), that refers that lack of cybersecurity can result in decreasing trust in the use of information and communication technology applying it on higher education institutions.

This study depends on measuring digital trust including three essential dimensions: technology used, people involved, and the digitalization process based on the scale of (Launer & Cetin, 2021; Launer et al., 2022). The average of users 'experience comes at first rank that interest of cybersecurity has a great impact on enhancing trust concerning users' experience (AV Mean= 4.45, SD= 0.358), followed by technology used (digital systems) (AV Mean= 4.37, SD= 0.418), and processes (AV Mean= 4.17, SD= 0.719). Regarding dimension of **Users' experience**, there is a strong agreement for all statements at (Mean= 4.45 SD= 0.358), as the most agreed statement is (There is no sharing of customers' personal data with others without obtaining the approval of their owners) at (Mean= 4.85 SD= 0.356), while the least agreed statements are (The user trusts that he can recover his data in a timely manner, and The website requests an evaluation of the provided services for continuous development of these services) at (Mean= 4.23, SD= 0.791), (Mean= 4.23, SD= 0.690) respectively.

Regarding dimension of **Technology used** (digital systems), there is a strong agreement for all statements at (Mean= 4.37, SD= 0.418), as the most agreed statement is (Information security programs enhance confidence in the system) at (Mean= 4.55, SD= 0.598), while the least agreed statements are (The company has policies and plans to enhance user confidence in its systems and programs, and Satisfaction of the overall performance of electronic services) at (Mean= 4.23, SD= 0.690).

Regarding dimension of **processes**, the high portion of respondents towards agree at (Mean= 4.17 SD= 0.719), as the most agreed statement are (Information security software

protects users' data from damage, and Information security programs limit the access of viruses to company devices) at (Mean= 4.55, SD= 0.669) (Mean= 4.40, SD= 0.768) respectively, while the least agreed statements are (The electronic payment process on the website is well secured, Information security programs reduce frequent email breaches, The company applies security standards to enhance protecting users' data) at (Mean= 3.96, SD= 1.000).

3.4. Hypotheses Test

3.4.1. First Hypothesis

This study assumes that there is a statistically significant difference among the opinions of the study sample regarding the interest of cybersecurity in Egyptian travel agencies. T- test was conducted for verifying this hypothesis, test's results are presented in the next table:

Table 7. One- Sample Test

Mean	Standard Deviation	Standard Error Mean	T- Test	95% Confidence interval for the two means		P-value(sig)
				Lower	Upper	
55.618	11.079	0.552	100.780	54.533	56.703	0.001

As shown in Table 7, the probability of significance (*P*) is lower than significance level (0.05) and that the tabulated value of T is lower than the calculated value of the T-test and hence the null hypothesis is rejected, and alternative hypothesis is accepted that: There is a statistically significant difference among the opinions of the study sample regarding the interest of cybersecurity in the Egyptian travel agencies.

3.4.2 Second Hypothesis

The study also assumes that there is an impact of cybersecurity on enhancing digital trust of travel agencies. Simple linear regression analysis and correlation were used to verify this hypothesis. simple linear regression was conducted for determining the effect of interest of cybersecurity on enhancing digital trust at a significance level (0.05) as shown in the next table:

Table 8. Simple linear regression analysis

Independent Variable	Beta β	T	T Sig.	R	R^2	F	F Sig.
Cybersecurity	0.586	14.472	0.001	0.586	0.343	209.446	0.001

Dependent variable: Enhancing Digital Trust

As shown in Table 8, (R^2): coefficient of determination refers that the independent variable (Cybersecurity) accounts for 34% of the change in the dependent variable (Enhancing Digital Trust). The values of F Sig. and T Sig. are lower than significance level (0.05), resulting to the rejection of the null hypothesis and acceptance of the alternative hypothesis that: There is an impact of cybersecurity on enhancing digital trust of travel agencies. The regression model is as following: Y= b0 + b1 X Enhancing Digital Trust= 49.026 +0.366 Cybersecurity

Correlation analysis was also conducted to examine the relationship between the two variables and for supporting the findings obtained from the regression analysis as shown in the following table:

Table 9. Correlation between Cybersecurity and Enhancing Digital Trust

Dependent Variable / Independent Variable	Enhancing Digital Trust	
Cybersecurity	Pearson correlation	0.586**
	Sig.(2-tailed)	0.000
	Spearman correlation	0.615**
	Sig.(2-tailed)	0.000

It is clear from table 9 that value of Pearson correlation coefficient (0.586) is statistically significant at the level of significance (0.01) with statistically significance (0.000), that refers to a direct correlation between the two variables. The Spearman correlation coefficient was also computed which is (0.615), that is statistically significant at the level of significance (0.01) with statistically significance (0.000), that also refers a direct relationship between variables. This means that if there is an interest of cybersecurity in travel agencies, the output will be enhancing digital trust.

Conclusion

The growing digital footprint of travel and tourism sector in the fourth industrial revolution results increasingly exposed to cyber threats either through online transactions, customer analytics, cloud integration, connected devices, or digital payment technology. This research aimed at enhancing awareness of the application of cybersecurity and clarifying the importance of cybersecurity in tourism and its role in reinforcing digital trust of travel agencies. Regarding analysis, it has been found that level of interest of cybersecurity in Egyptian travel agencies is to some extent, due to many reasons such as lack of training programs in cybersecurity for employees in travel agencies that threaten the cybersecurity of these institutions. That is consistent with the findings of other studies that the main reason for information security violations is due to employees' behavioural factors rather than technical issues per se, as employees are a key data security factor. Also, among these reasons nonexistence of a specialized department for information technology and cybersecurity in most of travel agencies, in addition to that, there is not enough strict administrative instructions about protecting the system from any fraud. That may lead to cyber risks in the travel and tourism sector if there is not enough attention about cybersecurity in travel agencies. Hence the negative consequences of breaches as, for example, losses of customer trust and deterioration of reputation put an emphasis on the importance of cybersecurity. The obtained results have shown that there is a positive impact of interest of cybersecurity on enhancing digital trust of travel agencies. As, building and maintaining trust in the digital field is an ongoing challenge that requires firm safeguarding of sensitive information and successfully resisting the attacks of malicious activities.

Limitations and Future research

The study focused on cybersecurity evidence from managers and employees in Egyptian travel agencies. Future research should examine the extent of awareness of practices of cyber hygiene which is related to cybersecurity but concerned to individuals representing clients of travel agencies. As well this study was applied on travel agencies in Arab Republic of Egypt, the future research suggested to be applied in different tourism entities as airlines and travel insurance firms.

Recommendations

According to both of literature review and findings of the field study, the following could be recommended to direct to travel agencies:

1- Allocating a specialized department for cybersecurity in travel agencies.
2- Need for strict administrative instructions about protecting the system from any fraud.
3- Creating data backups to reduce the impact of cyber-attacks.
4- Constantly updating software related to booking systems.
5- Investment in cybersecurity infrastructure for its role in achieving digital trust.
6- Increasing employees' awareness of cybersecurity through protocols for training employees in travel agencies by sustainable courses to develop their knowledge and skills.

References

Ahmed Abdel-Al, J., Al-Saeed Farrag, S., & Atwa Abdel-Hakim, R. (2022). Egyptian efforts to face cyber challenges. Scientific Journal of Environmental Studies, 13(2), 265-286.

Alghamdi, O. H., & Almostadi, W, A. (2021). The Role of Cybersecurity Application in Achieving Competitive Advantage – Field study on staff at King Abdelaziz International Airport in Jeddah, Journal of Economic, Administrative and Legal Sciences, 5 (9), 144-164

Al-Manea, A. (2022). Requirements for achieving cybersecurity in Saudi universities in light of Vision 2030. Journal of Faculty of Education, Assiut University, 38 (1), 155-194 (In Arabic).

Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber-attacks on hospitality sector: Stock market reaction. Journal of Hospitality and Tourism Technology, 11(2), 277-290. DOI 10.1108/JHTT-05-2019-0080

Bauernfeind, U., & Zins, A. H. (2006). The perception of exploratory browsing and trust with recommender websites. Information Technology & Tourism, 8(2), 121-136.

Bazazo, I., Al-Orainat, L., Abuizhery, F., and Al-Dhoun, R, A. (2019), Cyber Security Application in the Modern Tourism Industry. Journal of Tourism, Hospitality and Sport, Vol. 43, 46-55. DOI: 10.7176/JTHS

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

Biesiada J (2017) How to not fall victim to fraud. Travel Weekly, 22 Sept. https://www.travelweekly.com/Travel-News/Travel-Agent-Issues / Insights /Ways-to-not-fall-victim-to-fraud Accessed 20 December 2022

Borky, J. M., & Bradley, T. H. (2019). Protecting information with cybersecurity. Effective Model-Based Systems Engineering, Berlin: Springer International Publishing AG, 345-404.

Bridge M (2017) Russians buy life of luxury with stolen UK air miles. The Times, 21 Nov. https://www.thetimes.co.uk/edition/news/russians-buy-life-of-luxury-with-stolen-ukair-miles-psrkhqsfs. Accessed 25 August 2022.

Brook, C. (2018): What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More, Retrieved from digital guardian: https://www.digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more. Accessed on:17/07/2023.

Burns, S. and Roberts, L. (2013), "Applying the theory of planned behaviour to predicting online safety behaviour", Crime Prevention & Community Safety, 15 (1), available at: http://link.springer.com/article/10.1057/cpcs.2012.13 .

Cavelty, M. D. (2015). Cyber-security. In book: Contemporary Security Studies Chapter: 27, 4th Edition, Oxford University Press-UK , 401-416.

Chen, C. (2006). Identifying significant factors influencing consumer trust in an online travel site. Information Technology & Tourism, 8(3-4), 197-214.

Chen, H. S., & Fiscus, J. (2018). The inhospitable vulnerability: A need for cybersecurity risk assessment in the hospitality industry. Journal of Hospitality and Tourism Technology, 9(2), 223-234.

Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. Journal of information science, 44(6), 752-767.

Chui K.T. (2023) Building Digital Trust: Challenges and Strategies in Cybersecurity, Cyber Security Insights Magazine, Insights2Techinfo, Volume 5, 15-18.

Cybersecurity Ventures. 2020. "Cybercrime to Cost the World $10.5 Trillion Annually by 2025." Accessed on: 15March 2023 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

DeFranco, A. and Morosan, C. (2017): Coping with the risk of internet connectivity in hotels: perspectives from American consumers traveling internationally, Tourism Management, Vol. 61, 380-393.

Desku, A. (2002). Cyberattacks Increased by 60% In Tourism Sector This Year, 20 July, https://www.schengenvisainfo.com/news/cyberattacks-increased-by-60-in-tourism-sector-this-year/ Accessed on 19 September 2023.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

Ebrahim, F. A., Youssef, R., & El-said, W. M. (2022). Cybersecurity and Digital Cleanliness, Egyptian Journal of Information Sciences, 9(2), 390-422. (in Arabic)

El-Bishi, M. A. (2021): Cyber Security in Saudi Universities and its Impact on Enhancing Digital Confidence from Members Point of View: Study at Bisha University, IUG Journal of Educational and Psychology Sciences, 29 (6), 353-372 (in Arabic).

Farag, A, O, K., (2022):The Reasons for Promoting Cyber Security Culture in Light of Digital Transformation Prince Sattam Bin Abdulaziz University as a Model: International Journal of Educational Research, Sohag University-Egypt, 1(94), 509-537 (in Arabic).

Gordon, L.A., Loeb, M.P. and Lucyshyn,W. (2003). Sharing information on computer systems security: an economic analysis, Journal of Accounting and Public Policy, 22 (6), 461-485. https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Grabner-Kräuter, S. (2002), The Role of Consumers' Trust in Online-Shopping, Journal of Business Ethics, 39, 43-50.DOI: 10.1023/A:1016323815802.

Holdsworth, J. and Apeh, E. (2017): An effective immersive cyber security awareness learning platform for businesses in the hospitality sector, in Proceedings – 2017 IEEE 25th International Requirements Engineering Conference Workshops, REW 2017, IEEE, Lisbon, 111-117.

Hsu, C. H., & Kang, S. K. (2013). Buyer Characteristics Among Users of Various Travel Intermediaries. Handbook of Consumer Behavior, Tourism, and the Internet, 51-62

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2022). Maritime cybersecurity: are onboard systems ready?. Maritime Policy & Management, 1-19, DOI: 10.1080/03088839.2022.2124464

Kaspersky Lab (2018) Damage control: the cost of security breaches. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf. Accessed on 19 August 2022

Khari, M., Shrivastava, G., Gupta, S., & Gupta, R. (2017). Role of cyber security in today's scenario. In Detecting and mitigating robotic cyber security risks, pp. 177-191. IGI Global. DOI: 10.4018/978-1-5225-2154-9.ch013

Khwaldeh, S., Al-Hadid, I., Masa'deh, R., & Alrowwad, A. (2017). The association between e-services webportals information quality and ICT competence in the Jordanian universities. Asian Social Science, 13(3), 156-169.

Kovačić, M., Čičin-Šain, M., & Milojica, V. (2022). Cyber security and tourism: bibliometric analysis. Journal of process management and new technologies, 10(3-4), 75-92.

Launer, M. A., & Cetin, F. (2021). Exploring Digital Trust in Hotel Supply Chain: A Primary Research From the Hotel, Restaurant & Tourism Industry. Gloserv Conference 2021, University of Southern Florida, USA , 207.

Launer, M., Çetin, F., & Paliszkiewicz, J. (2022, March). Digital trust in the workplace: Testing a new instrument on a multicultural sample. In Forum Scientiae Oeconomia , 10 (1), 30-47.

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

Maguilo, A. (2016). Cyber Security and Tourism Competitiveness. EJTHR, Journal of Hospitality and Tourism Reserch, 7(2), 128-134.

Marcial, D., Launer, M. (2019), Towards the Measurement of Digital Trust in the Workplace: A Proposed Framework, International Journal of Scientific Engineering and Science, 3(12), 1-7. https://doi.org/10.5281/zenodo.3595295

McKnight, D.H., Choudhury, V., Kacmar, Ch. (2002), Developing and validating trust measures for e-commerce: An integrative typology, Information Systems Research, 13(3), 334-359. DOI: 10.1287/isre.13.3.334.81.

Olson P (2019). Marriott faces $124 million fine over Starwood data breach. The Wall Street Journal, 9 July. https://www.wsj.com/articles/marriott-faces-123-million-fine-over-starwooddata-breach-11562682484. Accessed on 25 July 2023.

Öztüren, A. (2013). Effects of electronic trust on purchase intentions in online social review networks: The case of TripAdvisor. com Life Science Journal, 10(2), 2002-2010.

Paraskevas, A. (2022). Cybersecurity in travel and tourism: a risk-based approach. In Handbook of e-Tourism (pp. 1605-1628). Cham: Springer International Publishing.

Pietrzak, P., Takala, J. (2021), Digital trust –a systematic literature review, Forum Scientiae Oeconomia, 9(3), 59-71. https://doi.org/10.23762/FSO_VOL9_NO3_4

Rodríguez-deArriba, M. L., Nocentini, A., Menesini, E., & Sánchez-Jiménez, V. (2021). Dimensions and measures of cyber dating violence in adolescents: A systematic review. Aggression and Violent behavior, 58, 101613.

Ruzic, V., & Matika, D. (2020). Cybercrime and Protection of Business Information in Tourism Industry-Croatian Perspective. Economic and Social Development: Book of Proceedings, 98-108.

Schatz, Daniel; Bashroush, Rabih; and Wall, Julie (2017). Towards a More Representative Definition of Cyber Security, Journal of Digital Forensics, Security and Law: 12 (2) , Article 8. DOI: https://doi.org/10.15394/jdfsl.2017.1476

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. john wiley & sons.

Singh, D., Mohanty, N. P., Swagatika, S., & Kumar, S. (2020). Cyber-hygiene: The key concept for cyber security in cyberspace. Test Engineering and Management, 83, 8145-8152.

Tan, Y.H. and Thoen, W. (2001). Toward a generic model of trust for electronic commerce. International Journal of Electronic Commerce, 5 (2), 61–74.

Tawfiq, S. M. & Mousa, S. E. (2023).Requirements for achieving cybersecurity in Egyptian universities In light of the digital transformation from the point of view of faculty members, Journal of Education-Sohag University, 2(105) ,738-866 (In Arabic).

The Egyptian Travel Agents Association (ETTA) (2023) at https://www.etaa-egypt.org/SitePages/CompaniesStatistics.aspx, Accessed on 26 June 2023

Van Bogaert, D. K., & Ogunbanjo, G. A. (2009). Confidentiality and Privacy: What is the difference?. South African Family Practice, 51(3), 194-195. DOI:10.1080/20786204.2009.10873845

Van Selm, M., & Jankowski, N. W. (2006). Conducting online surveys. *Quality and quantity*, *40*, 435-456.

Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. European Journal of Sustainable Development, 7(4), 171-178.

Vishwanath, A., Neo, L. S., Goh, P., Lee, S., Khader, M., Ong, G., & Chin, J. (2020). Cyber hygiene: The concept, its measure, and its initial tests. Decision Support Systems, 128, 113160.


مجلة اتحاد الجامعات العربية للسياحة والضيافة
(JAAUTH)
الموقع الإلكتروني: http://jaauth.journals.ekb.eg/


استكشاف دور الأمن السيبراني في تعزيز الثقة الرقمية لوكالات السفر والسياحة المصرية

ريهام ممدوح عبد المقصود

قسم الدراسات السياحية – كلية السياحة والفنادق – جامعة المنصورة–مصر

معلومات المقالة

الكلمات المفتاحية

الأمن السيبراني؛
النظافة السيبرانية؛
الثقة الرقمية؛
وكالات السفر.

(JAAUTH)
المجلد ٢٦، العدد ١، (٢٠٢٤)، ص ١٨٥-٢٠٤.

الملخص

نظرًا لأن قطاع السفر والسياحة أصبح يستخدم بشكل متزايد مختلف التقنيات، فإن الأنظمة البيئية السيبرانية الخاصة بهذا القطاع أصبحت معرضة بشكل متزايد لمخاطر السلامة والأمن المرتبطة باستخدام مثل هذه التقنيات. وعلى الرغم من وجود الكثير من الأدلة التي تشير إلى تزايد تعرض أنظمة السفر والسياحة لتهديدات الأمن السيبراني، إلا أن الأدبيات المطبقة على قطاع السياحة لا تزال محدودة. ومن هنا فيهدف هذا البحث إلى تعزيز الوعي بتطبيق الأمن السيبراني والنظافة السيبرانية التي ترتبط بها، وتوضيح أهمية الأمن السيبراني في السياحة ودوره في تعزيز الثقة الرقمية لوكالات السفر. فقد تم تصميم استبيان وتوزيعه على عينة عشوائية بلغ عددها ٤٠٣ من المديرين والموظفين المعنيين في وكالات السفر المصرية للتعرف على مدى الاهتمام بالأمن السيبراني في وكالات السفر المصرية ودوره في تعزيز الثقة الرقمية، وقد تم تحليل تلك الاستجابات باستخدام برنامج SPSS إصدار 28. وقد أسفرت نتائج البحث أن وكالات السفر المهتمة بالأمن السيبراني يمكنها تعزيز الثقة الرقمية لعملائها. وأوصى البحث بضرورة اكساب الموظفين المهارات اللازمة لتحقيق الأمن السيبراني، وضرورة وجود قسم مختص بالأمن السيبراني، واتخاذ الاجراءات اللازمة لتحقيق الوقاية والحماية للشبكات السياحية للدور الفعال في تحقيق الثقة الرقمية لوكالات السفر.