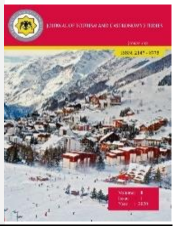
JOURNAL OF TOURISM AND GASTRONOMY STUDIES

ISSN: 2147 – 8775

Journal homepage: www.jotags.org



The Importance of Information Security in Travel Enterprises: Kuşadası Case

*** Kamil YAĞCI [a], Süreyya AKÇAY [b], Mahmut EFENDİ [c]**

[a] Pamukkale University, Faculty of Tourism, Department of Tourism Guidance, Denizli/Turkey
[b] Gazi University, Institute of Social Science, Department of Tourism Management, Ankara/Turkey
[c] Adnan Menderes University, School of Tourism and Hotel Management, Department of Travel Management and Tourism Guidance, Aydın/Turkey

Article History

Received: 24.02.2020

Accepted: 26.03.2020

Keywords

Information
The importance of information
Information security
Travel enterprises
Tourism

Abstract

In society today, the value and security of information is a remarkable issue for all individuals and enterprises. Individuals have doubts about the security of this information while using their personal information. Besides, the enterprises carry out practices on the security of the information they obtain. The purpose of this study is to understand the views of the executives of travel enterprises that are within the scope of tourism enterprises regarding information security and what efforts are made for the information security of the enterprises. It is acknowledged in line with the study conducted for this purpose that the executives of travel enterprises are worried about the security of their own information but do not use international information security systems even though they make great effort in order to ensure that the information they have obtained in their enterprises do not get in the hands of others.

Article Type

Research Article

******* *Corresponding Author*
E-mail: kyagci@pau.edu.tr (K. Acar)

DOI: 10.21325/jotags.2020.565

INTRODUCTION

In the twenty-first century, the widespread use of information technologies by the individuals, companies, institutions and all the segments of the state requires the development of effective policies regarding security (Eminağaoğlu & Gökşen, 2009). With the increase in the use of information technologies, problems about the security of these technologies have become extremely significant.

Together with the fact that providing information and using information technologies is a necessity of the enterprises and workplaces, they need to rely on this information they obtain (Kruger & Kearney, 2006). The number of internet users worldwide is more than 4 billion today (www.worldometers.info). As the number of internet users is increasing gradually day by day, the works and operations carried out by the world population takes a wide place in the digital environment and therefore, it is required that the enterprises also perform on the internet.

Since information is accepted as the most important production factor (Acılar, 2009), the enterprises have been able to manage their abilities effectively through using the communication opportunities that differ with the development of information technologies (Mestçi, 2007). There are still many shortcomings in the effective management of this form of communication (Canbek & Sağıroğlu, 2006). The use of information technologies provides plenty of benefits like speeding up in tasks and operations, saving time, reaching large masses, and transparency. Benefiting from the positive aspects of information technologies raises the problem of information security in digital settings (Alagöz & Allahverdi, 2011; Yavanoğlu, Sağıroğlu & Çolak, 2012).

Although the problems regarding the protection of information are worrying, life without information technologies seems almost impossible. For this reason, the widespread use of information technologies has become a necessity since the protection of information has become an obligation as the threats have been increasing (Henkoğlu & Yılmaz, 2013). In the event that the security of information platforms is not provided, it is possible to mention various information security problems such as releasing the confidential information and commercial secrets of the institutions, illegal operations, labor losses caused by accidents and disasters, material and spiritual (such as dignity) losses (Eminağaoğlu & Gökşen, 2009).

Information security is related to a number of measures taken to prevent the access, use, transfer, alteration or destruction of those who are not authorized (Baykara, Daş & Karadoğan, 2013). These measures protect the ones using the information from the deficits that may arise from the confidentiality of information, protection of integrity and identification of access options. Information security processes of the organizations also include the processes in which all organization employees are responsible, not only the IT specialists with technical knowledge (Johnson & Goetz, 2007; Acılar, 2009). The elements that threaten the protection of information stem from the wrong work and behaviors of the employees within the organization rather than the external factors and therefore, studies should be carried out so as to inform the employees (Acılar, 2009).

The institutional information pools that organizations obtain through information technologies are also important, broad assets that are open to threats and that require management support to be protected. One of the sectors involving comprehensive information is the tourism sector (Marşap, Akalp & Yeniman, 2010; State Supervisory Board, 2013). The protection of the confidentiality, accessibility and integrity of information is a vital issue that concerns the whole organization from the lowest level to the highest (Tekerek, 2008). One of the organizations that are involved in the tourism sector and that perform mostly through information technologies is travel agencies. In this study, it is aimed to determine the awareness of travel agency executives regarding the security of information and what kind of tasks and operations they carry out in order to keep their information secure. The study was completed according to qualitative research methods design via the interviews with the managers at the travel agency. Interview, which was selected as the qualitative data collection technique, was prepared in the semi-structured manner. In this respect, interviews were conducted with 12 travel agency managers within the framework of the study.

Theoretical Framework

Data, Information and Knowledge

The development of information technologies and the internet have become the most effective means of communication and the greatest sources of information in this century. As a result of these developments, the tourism sector has become an important source of information with extensive information pools (Giritlioğlu, 2014). The use of these resources involve the management processes that require self-knowledge and human factors (Grover & Davenport, 2001; Canbek & Sağıroğlu, 2006).

"Data" can be defined as "the convenient presentation of phenomenon, concepts or commands for communication, interpretation and processing" (Türk Dil Kurumu [Turkish Language Association], 2018) or "in terms of information technology; the known assets whose connections have not been established yet, or briefly, the signals and/or bit strings found and transmitted in digital environments" (Canbek & Sağıroğlu, 2006).

Information is obtained by making the raw data meaningful. In order for some information to be valuable, it should be in interaction with other information (Gürcan, 2014). *Knowledge* is about the understanding and awareness of information (Canbek & Sağıroğlı. 2006).

Information and Information Security

Internet is the digital setting in which individuals provide information exchange for both commercial and individual purposes (Alagöz, 2007; Alagöz & Allahverdi, 2011). In order to provide information security in these settings (technical, legal, etc.), evaluations should be made in many dimensions (Henkoğlu & Yılmaz, 2013). According to Doğantimur (2009), information security is the protection of the confidentiality, integrity and accessibility of information. According to Tatar (2015), information security means that confidential information can only be saved and accessed by authorized persons. Integrity is the prevention of information without being corrupted, changed or erased. Besides, accessibility refers to easy access to information by authorized persons.

Ensuring information security can be achieved through the fulfillment of the confidentiality, integrity and accessibility of information. The violation of these three elements by unauthorized individuals raises the threats so-called as "cyber security incident or cyber-attack" (Kara, 2013). These threats require taking preventative measures as they can cause harms (Bağcı, 2016). The malevolent people who are perceived as threats here are called the opposing party (attackers or cyber terrorists). In order to prevent the damage that may be caused by the opposite party, security policies should be established, the accesses should be monitored, and the changes and deletions should be reported and limited (Canbek & Sağıroğlu, 2006). Securing information through these steps will increase the profits by eliminating security problems (Ganbat, 2013). It is possible to classify these threats to information resources as human-based threats, physical threats, software-based threats and vulnerability, lack of education, and unconsciousness (Tekerek, 2008).

The Importance and Protection of Information Security

The use and dissemination of the internet draws the attention of some malevolent people who may acquire some gains through the flow of information. Unauthorized access to information resources makes it possible to steal, destroy, erase and alter or even sell information. For example, the fact that the vital information of almost 500.000 websites were stolen because of the security gap called Heartbleed (the security gap that makes it possible to access the encrypted information) is one of the most significant security incidents in the world (Siber Güvenlik Derneği [Cyber Security Association], 2014). On the other hand, it is known that plenty of financial gain was obtained with the cyber security incident called cryptolocker that enables the access to information through fake e-mails such as the e-mails of official institutions, which is also a method widely used in Turkey (Cyber Security Report, 2014; https://www.uab.gov.tr/). Furthermore, Annoymus, one of the hacker groups that performs hacking events for many reasons but especially to attract attention, announced through social media that the information of Turkish Police Department was hacked (https://www.milliyet.com.tr/teknoloji/hacklenen-emniyet-sitesinin-komik-sifresi-1511863).

No matter it is a public institution or a private sector enterprise, every institution may experience cyber-attacks and therefore, they have to create their own information security policy. One of the settings that makes extreme information sharing and is affected by cyber events is the web contents created by tourism enterprises (Chen, Chu & Wu, 2012). Among the web contents that attract attention most in terms of providing access, the contents related to tourism has a remarkable place (Karamustafa & Öz, 2010). This situation caused such big companies as THY (Türk Hava Yolları [Turkish Airlines] and IETT (İstanbul Elektrikli Tramvay ve Tünel İşletmeleri [Istanbul Electricity Tramway and Tunnel Establishments], which are of the significant transportation companies in Turkey, to undergo cyber-attacks, experience panic, reputation loss and financial loss (www.trtturk.com; http://www.mynet.com/iett-hacklendi-110102367277).

Today, as ensuring the security of information in digital settings has been the most fundamental requirement of individuals and institutions, high level measures should be taken against cyber-attack incidents that may be experienced. The losses created by the deficiencies that may occur in these settings due to the immediate access to information from anywhere and at any time make in-house physical, software-based or human-based measures mandatory (Vural & Sağıroğlu, 2008; Çetinkaya, 2008).

In order to ensure information security, it is necessary to provide the confidentiality of information which is related to the access of only those related to the information, and the integrity of information, which is related to keeping the information as it actually is without making a change, not deleting or destroying it. Besides, it is necessary to make the accessibility available so that the accessibility of information can only be done by authorized persons (Hekim & Başıbüyük, 2013). This makes the executives of information systems responsible for ensuring information security as well as the owner of information and the user of information. The actual purpose of information security is to ensure that the right person reaches the right information within the shortest time (Henkoğlu & Yılmaz, 2013). Therefore, while planning to take the necessary measures to ensure the security of information, the executives should implement practices that take into account the human factor, which is the most important factor in ensuring the information security (Acılar, 2009). The main reason for this is that the threats created by the employees of the organizations who are called as internal threats both consciously or unconsciously constitute a remarkable amount among information security threats (Baykara, Daş & Karadoğan, 2013). The way to ensure information security is, first of all, to establish an Information Security Management System. With the support of senior management, a project team should be established and the implementation of the information security management system policy should be provided within the institution (Çetinkaya, 2008).

International standards aim to protect the information resources at the international level by undertaking the necessary mission in the creation and implementation of information security policies. Regarding the issue, the British Standards Institution put a stake on the ground by issuing the BS7799 standard in 1999, and developed the ISO/IEC 17779 standard with ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission). Furthermore, the same institutions developed ISO 27000 standard series which are still current today, integrated and rearranged the previous standards in 2005 and these series of standards have begun to be implemented (Başaran, 2016; Fenz et al. 2007; Guan, Lo, Wang & Hwand, 2003).

In Turkey, following these developments, ISO 27001 Standard was translated into Turkish language by TSE (Türk Standartları Ensitüsü [Turkish Standards Institution] and it was launched under the name of TSI ISO/IEC 27001 (Ganbat, 2013). This standard, which can be used by all organizations, is a guide to protect information, manage the threats accurately and ensure the continuity of the established security system (Başaran, 2016). Besides, in order to ensure the security of the systems developed for card payment, Payment Cards Industry Data Security Standard (PCIDSS) has been established, which has pioneers as American Express and Mastercard, which is supervised by the firms authorized by the Payment Cards Industry (PCI Council), and which is formed of the procedures that are responsible for the information security of individuals and institutions using these standard card systems (Lovrić, 2012; Susanto, Almunawar & Tuan, 2011).

Keeping up with information security procedures protects information against threats and determines the limits of authority against arbitrary practices and information leaks within the organization. In addition to the information security management systems, digital tracking systems regarding the protection and sharing of confidential information and documents should even be put into practice (Kaya, 2015).

Information Security in Travel Agencies

The rapid changes in information technologies after the 1950s made computers an indispensable part of human life (Çetinsöz, 2015). The development of internet and the growth of internet use in the entire world has had a significant impact on the traditional sale of tourism and travel services just as in other industries, and these products have reached significant sales rates over the internet. In the tourism industry, which is a remarkable part of global trade, internet has been used for many different purposes for a long time (Sarıışık & Akova, 2006). Web sites are generally used in the social communications performed through the internet. These websites are called social networking websites (Erdoğan & Bahtiyar, 2014).

Ensuring the security of information is possible by implementing certain measures that can be taken by analyzing the certificates, standards or risks (Aktaş & Soğukpınar, 2010; Diker & Varol, 2013). The enterprises providing online services improve customer relations by distributing large-scale information and provide significant benefits in terms of forming large customer database and developing after-sales services (Barnes & Cumby, 2002; Diker & Varol, 2013). The travel agencies, which mediate the supplier-customer relations between the travelers and the enterprises to be accommodated, carry out transactions with information and information resources rather than physical products. For example, the information of age, gender, marital status, income, etc. obtained from the customers by the travel agencies provides competitive advantage by giving information on many topics about those wishing to travel such as the hobbies they wish to try or the travel locations they would like to choose on their next trip (Yıldız & Yıldız, 2015). For this reason, travel agencies are one of the areas of tourism industry that necessitate information security issues most.

Travel agencies also affect the quality of service perceived by the customers with the services they provide. In their study on e-travel service quality, Ho and Lee (2007) revealed that "security" and "information quality" sub-dimensions significantly affected the quality of e-service in the sub-dimensions of "web functionality", "customer relations" and "accountability".

The widespread use of information technologies enables the emergence of conscious and independent consumers, the creation of search engines (such as Google, Yandex) where they can make their own travel decisions, and the widespread use of e-travel platforms or mediating websites that compare travel options (Musafir.com, Travelocity, Trivago) (Buhalis & Law, 2008; Yıldız & Yıldız, 2015). When the content and functionality of the web page, and the presence of information security provided by the web page in the purchases made through e-agencies are analyzed through the consumer perspective, it is revealed that it has positive effects on the perceived value of online tourism service and the continuity of purchase intention (Liao & Shi, 2017).

Through information technologies, travel enterprises increase their efficiency and productivity, and find opportunities to develop many innovative strategies except from traditional marketing methods (Buhalis, 1998; Doğan & Morkoç, 2015). Lin and Fu (2012) determined that the necessary criterions for consumers' adoption of internet-based sales that the travel agencies perform for the purpose of acquiring a competitive advantage by using information technologies are the content of the product information and the security of e-trade system.

All the services such as having online information about a location that the consumer who wishes to have a holiday, evaluating alternative accommodation and transportation opportunities, making reservations, and paying quickly and safely are possible with the services of travel agencies. Travel enterprises, just like many other enterprises in tourism, aim to create their own customer masses by establishing their own reservation and communication systems over the internet. Therefore, the services provided are being accelerated, price alternatives are being made available, security measures are being increased and the connection between tourism sector and internet is being strengthened (Türker & Türker, 2013).

Method

Research Method

Due to the need to study on a group or population, to identify the variables that cannot be measured easily or to hear the silenced sounds, exploratory research arises and it is said to be the best way to discover a problem rather than using the predetermined information in the literature because qualitative research is carried out in order to bring a detailed understanding of a complex subject (Creswell, 2016). Qualitative research is an approach that focuses on searching and understanding social phenomenon in their related environment with an understanding based on forming theory. In this definition, “theory formation” means a modeling study that explains the previously unknown results in relation to each other based on the information collected (Yıldırım, 1999). Qualitative research is a research type in which the researcher investigates the subject or event in its natural environment and tries to determine and interpret the meanings that the researched individual has structured in their mind about these situations (Denzin & Lincoln, 1998). The research questions prepared in this study are shaped according to phenomenology design, which is of the qualitative research designs. The main purpose in phenomenology studies is to focus on the phenomenon that is recognized but is not known with a deeper and detailed understanding (Büyüköztürk et al., 2015; Bal, 2016).

Observation and interview, which are of the qualitative research methods, are aimed at catching and understanding this relativity and mobility of social phenomenon. The most remarkable advantages of these methods are to allow the subject of the research to be seen from related people’s perspectives and to reveal the social structure and processes constituting these perspectives (Yıldırım, 1999). In qualitative research, the time, energy, organization and money required to collect the data of the interviews and observations necessitates to keep the sample limited. Furthermore, the intensity and abundance of the data obtained through observations and interviews play an important role in this selection process. It is a common practice in qualitative research to transcribe an interview which lasts for half an hour to a few hours and obtain meaningful themes from the transcribed interview text or data regarding the research problem. Therefore, the sample size in qualitative research cannot reach the sample size in quantitative research most of the time (Yıldırım & Şimşek, 2006).

Interview is one of the main data collection tools in qualitative research and is one of the most frequently used research methods in social sciences (Yıldırım & Şimşek, 2006). Interview is the discussion between two or more people for a specific goal. Generally, interviews can be classified as structured, semi-structured or unstructured interviews. Structured interviews are the interviews formed of a predetermined set of standardized questions (Berg & Lune, 2015). Unstructured interviews are conducted to reveal the existing information on a general field and do not involve a predetermined set of questions. Semi-structured interviews have a road map in general but they seek to reveal the different dimensions of the subject by asking different questions within this general framework according to the interest and knowledge of the respondent (Altunışık et al., 2007; Üzümcü, 2015).

The Purpose of the Research

The starting point of the research is the research questions and they are presented as the first determining point of design. The Questions prepared by the researchers. The aim of this study is to reveal the views of the individuals working as the executives of the travel agencies in Kuşadası regarding information security. For this purpose, the answers are sought for the questions below.

- Do executives have any information regarding information security?
- Have executives taken any institutional measures to ensure the security of their enterprises’ information? (No/Why not? – Yes/What measures?)
- Do executives have any information about ISO 27001, which is an international data security standard? Do they consider that such a system will contribute to their enterprises?

- What are the executives thinking about the negative developments regarding information security (they may have heard about the incidents like cyber-attacks, data thefts, and hacks) encountered in Turkey and in the world?
- Do the executives use their personal information on the internet? (Such as credit card, password, birthday, national ID number, etc.) (Why? How often?)
- According to executives, are their computers and information safe? Do they take any measures to ensure their security? If not, why not?

The Population and Sample of the Research

The data source of the research was composed of the individuals who had experienced the phenomenon that the research focused on and who could reflect the phenomenon. For this reason, the population of the research was composed of the individuals in the managerial positions of the travel agency. As there were such constraints as time and financial constraints in reaching the whole population, sampling was preferred in conducting the research and in this study, which was carried out by using purposeful sampling method, the open-ended question form was completed by reaching 12 travel agency owners or executives. In this respect, face-to-face interviews were conducted with 12 travel agency owners or executives within the framework of the study. The face-to-face interviews completed nearly 50 minutes or 1 hour. The research was conducted between 1st of June and 1st of October in 2018 in Kuşadası due to easy access to the individuals working in managerial positions at the destination.

The data of the research was collected with an open-ended question form involving 6 structured questions. In order to analyze the data obtained from the responses that the executives give to the question form prepared in Turkish language, computer-aided content analysis was performed. Content analysis is a holistic analysis including data coding, finding the themes, organizing the codes and themes, and identifying and interpreting the findings (Bal, 2016). The findings obtained as a result of the frequency and percentage analysis through content analysis were put in the order of importance and the intensity and importance of the elements were tried to be revealed (Karadağ, 2010).

Findings

The demographic characteristics of the individuals participating in the research who were the owners or executives of the travel agencies are presented first and then, the questions asked to these participants are given in the tables below.

When the ages of the participants were examined, it was revealed that 3 executives were 30 years old or below (25%), 5 executives were between 31-35 years of age (41,67%), 3 executives were between 36-40 years of age (25%), and 1 executive was between 46-50 years of age (%8.33) type. In addition to this, when the genders of the participants were analyzed, it was found that there were 6 male executives (50%) and 6 female executives (50%). When educational status of the participants in the research was examined, it was revealed that 3 of the participants (25%) were high school graduates, 8 of them (66.67%) were university graduates and 1 of them (% 8,33) had postgraduate degree. Furthermore, when education field of the participants were analyzed, it was seen that 9 executives (75%) had education in the field of tourism and 3 of the executives (25%) did not have education in the field of tourism. Finally, to the question of how many years they had been working in this field, 1 participant (8,33%) gave the answer of 1-5 years, 3 participants (25%) gave the answer of 6-10 years, and 8 participants (66,67%) gave the answer of more than 10 years.

The answers given by the participants to the question “Do you have any information regarding information security?” are shown in Table 1 below.

Table 1. The findings regarding whether the executives have any information about information security

Views	Frequency	Percentage
Yes, I do.	12	100

All the executives participating in the research (%100) stated that they had information regarding information security.

Some of the responses given to the question of “Do you have any information regarding information security?” are given below.

R 8. “It is the protection of the security of information.”

R 9. “It is that the users can access the data they require immediately and safely whenever they need.”

R 12. “It is the protection of the computer and data.”

The answers given by the participants to the question “Have you taken any institutional measures to ensure the security of your enterprise’s information?” are shown in Table 2 below.

Table 2. The findings regarding whether the executives have taken institutional measures for information security

Views	Frequency	Percentage
Yes, I have (digital signature, antivirus, trainings, institutional identity, firewall, encoding action, electronic approval, cloud disk).	11	91.67
No, I haven’t.	1	8.33

To the question of “Have you taken any institutional measures to ensure the security of your enterprise’s information?”, almost all the participants [11 participants (91,67%)] responded having taken measures and just 1 participant (%8.33) responded not having taken any measures, and some of the responses are given below.

R 1. “We receive support in terms of information storage and security through an agreement with a private software company.”

R 2. “We protect our data in virtual setting (cloud disk) in a secure way.”

R 9. “We have an IT specialist working for our enterprise.”

The answers given by the participants to the question “Do you have any information about ISO 27001, which is an international data security standard? Do you consider that such a system will contribute to your enterprise?” are shown in Table 3 below.

Table 3. The findings regarding whether the executives have information about İSO 27001 standard

Views	Frequency	Percentage
Yes, I do (Apart from this, there are also some other data systems. I believe they will also contribute, maybe we will use in the future).	6	50.00
No, I don’t.	6	50.00

Some of the responses given to the question of “Do you have any information about ISO 27001, which is an international data security standard? Do you consider that such a system will contribute to your enterprise?” are given below.

R 2. "In addition to an international data security system, there are also data security systems produced by different companies."

R 3. "Yes, I do. I believe it will contribute to our enterprise. It would be better for us and for our customers."

R 9. "By means of performing information security in ISO 27001 standards, only those who are authorized can access the system, this enriches the enterprise and the information protected gives trust to its owner."

The answers given by the participants to the question "What are you thinking about the negative developments regarding information security (you may have heard about the incidents like cyber-attacks, data thefts, and hacks) encountered in Turkey and in the world?" are shown in Table 4 below.

Table 4. The findings regarding the views of the executives about the developments in terms of information security.

Views	Frequency	Percentage
I have negative thoughts (data theft and misuse requires attention. It is not secure; passwords should be renewed continuously. Technical infrastructure is important; strong programs are required, legal measures are required, for the threats coming with technology necessitates user trainings, the information obtained for many years should be preserved).	12	100

All the responses (100%) given to the question of "What are you thinking about the negative developments regarding information security (you may have heard about the incidents like cyber-attacks, data thefts, and hacks) encountered in Turkey and in the world?" are, in a way, as "I have negative thoughts", and some of the responses given are as follows.

R 4. "It is necessary that the information gathered difficultly for years should be stored and protected very well."

R 7. "Data theft, I mean, not being able to protect data is a bad and risky situation both for the enterprise and customers."

R 9. "By providing continuous trainings for the employees within the institution regarding the protection of information, information security should be provided."

The answers given by the participants to the question "Do you ever use your personal information on the internet? (Such as credit card, password, birthday, national ID number, etc.) (Why? How often?)" are shown in Table 5 below.

Table 5. The findings regarding whether the executives share personal information online

Views	Frequency	Percentage
Yes, I do (for shopping online and banking transactions, due to lack of time).	12	100

All the executives participating in the research (%100) stated in their responses to the question of "Do you ever use your personal information on the internet? (Such as credit card, password, birthday, national ID number, etc.) (Why? How often?)" that they shared their personal information. In addition to this, to the question of "How often do you do shopping online?", 1 executive (8.33%) responded that 6-8 times a month, 4 executives (%33.33) responded that 9-13 times a month, 3 executives (%25) responded that 14-18 times a month, and 4 executives (33.33) responded that 19 times a month and more.

The answers given by the participants to the question "Do you think your computer and information are safe? Do you take any measures to ensure their security? If not, why not?" are shown in Table 6 below.

Table 6. The findings regarding the views of the executives about the security of their information

Views	Frequency	Percentage
No, I don't (encoded login, I renew the password, I do not read unsafe e-mails, professional software, antivirus, banking transactions).	9	75
Yes, I do (antivirus, firewall, avast)	3	25

To the question of "Do you think your computer and information are safe? Do you take any measures to ensure their security? If not, why not?", most of the participants [11 participants (75%)] responded that they were not safe, and just a few participants [5 participants (25%)] responded that they were safe.

R 5. "They are not safe. Although I use antivirus programs and I do data backup, more secure systems are required."

R 8. "They are not safe. As I have just learnt, international programs are required."

R 10. "They are safe. I do not use them after work. I have antivirus programs and firewall."

Conclusion, Discussion and Suggestions

Today, individuals do their shopping online more quickly in virtual settings due to lack of time. With the development of information technologies, information sharing over the internet, which has increased as a result of the widespread use of mobile communication devices in recent years, raises the problem of information security.

In this study, awareness about information security was aimed to be created in travel agencies, one of the tourism industry stakeholders using information and communication technologies in each process of their activities because the information that is not secure affects the trust that individuals put in the institutions and organizations, and this may cause many financial and spiritual losses.

In addition to taking the necessary measures to be able to acknowledge the importance of information security, efforts should be made to raise awareness, the trainings of information technology users should be provided, and academic studies regarding the subject should be increased. In order for the information to be protected, the enterprises should also treat consciously as well as the consumers benefiting from the services provided by the tourism enterprises in virtual settings, and the enterprises should inform their stakeholders by taking the necessary measures in such fields as software, hardware and management. It should be remarkably noted that those who activate information technologies are the human factor although they seem to be threatening and malevolent software.

What can be said for future studies is to carry out studies with customers primarily to see the effects of information sharing in the field of tourism. In addition to this, in the study conducted, 12 owners or senior executives of travel agencies were interviewed and it was thought as a result of the study that it would also be an effective research to reveal what low-level employees were thinking about this issue. The study conducted was completed according to qualitative research design and therefore, it would be helpful for us to have knowledge about certain subjects in further studies to be conducted using quantitative methods. It is also understood that only a small number of individuals know the presence of a world-standard information security system and that due to the strengths of this system, the protection of the information of travel agencies will be made in a healthier way if a good promotion is made.

As can be understood from this research, travel agencies are only trying to protect the security of their information by implementing simple methods regarding information security. Together with the trainings to be carried out under the leadership of the Association of Turkish Travel Agencies, it can be revealed as an undeniable fact that information security of the sector will be learnt more quickly and customers' trust will be increased.

REFERENCES

Acılar, A. (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon Ve Yönetim Bilimleri Dergisi , 1(1),* 25-33.

Aktaş, F. Ö., & Soğukpınar, İ. (2010). Bilgi güvenliğinde uygun risk analizi ve yönetimi yönteminin seçimi için bir yaklaşım. *Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3(1),* 39-46.

Alagöz, A. (2007). Web sitesi maliyetlerinin muhasebeleştirilmesi. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , (18),* 11-24.

Alagöz, A., & Allahverdi, M. (2011). Kurumsal bilgi güvenliği ve muhasebe bilgi sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi , 4(3),* 47-64.

Altunışık R., Coşkun R., Bayraktaroğlu S. & Yıldırım E. (2007). *Sosyal Bilimlerde Araştırma Yöntemleri-SPSS Uygulamalı*, Sakarya: Sakarya Yayıncılık.

Bağcı, B. (CISA, 13 Mart 2016). Bilgi teknolojileri risk yönetimine genel bakış, . http://www.denetimnet.net/UserFiles/Documents/DeloitteMakaleleri/Bilgi%20Teknolojileri%20Risk%20Y%C3%B6netimine%20Genel%20Bak%C4%B1%C5%9F.pdf. Accessed: 21.03.2019.

Bal, H. (2016). *Nitel Araştırma Yöntem ve Teknikleri*, İstanbul; Sentez Yayıncılık.

Başaran, B. (2016). The effect of ISO quality management system standards on industrial property rights in Turkey. *World Patent Information, 45,* 33-46.

Barnes, J. G. & Cumby, J. A. (2002). Establishing customer relationships on the Internet requires more than technology. *Australasian Marketing Journal (AMJ), 10(1),* 36-46.

Baykara, M., Daş, R. & Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. E. Üniversitesi (Dü.), *1 International Symposium on Digital Forensics and Security inside,* 231-239, Elazığ.

Berg, L. B. & Lune, H. (2015). *Sosyal bilimlerde Nitel Araştırma Yöntemleri* (Bulut, Y. & Ercan B., Nitel Araştırmayı Desenleme inside Translate.), 37-80.Konya: Eğitim Yayınevi.

Buhalis, D. (1998). Statejik use of ınformation in the tourism industry. *Tourism Management , 19 (5),* 409-421.

Buhalis, D. & Law, R. (2008, August). Progress ın ınformation technology and tourism management: 20 years on and 10 years after the internet the state of eTourism research. *Tourism Management , 29 (4),* 609-623.

Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. & Demirel, F. (2015). *Bilimsel Araştırma Yöntemleri* (Improved 19th Edition). Ankara: Pagem akademi yayınları.

Canbek, G. & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi , 9 (3),*165-174.

Chen, A. H. C., Chu, H. C., & Wu, S. C. (2012). Against the breaches: data loss prevention for online travelling services. In Information Security And Intelligence Control (ISIC), *International Conference on,* 282-285.

Creswell, J. W. (2016). *Nitel Çalışma Tasarımı.* (M. Bütün, & S. B. Demir içinde, Nitel Araştırma Yöntemleri (A. Budak, & İ. Budak, Çev.), Cilt 3, 42-68. Ankara: Siyasal Kitabevi.

Çetinkaya, M. (2008). Kurumlarda bilgi güvenliği yönetim sistemi'nin uygulanması. Akademik Bilişim 2008 Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, 30 Ocak - 01 Şubat 2008 (511-516), Çanakkale Onsekiz Mart Üniversitesi, Çanakkale.

Çetinsöz, B. C. (2015). Yerli turistlerin satın alma eğilimlerinin teknoloji kabul modelinde analizi (TKM). *Elektronik Sosyal Bilimler Dergisi , 14 (53),* 242-258.

Denzin, N. K. & Lincoln, S. Y. (2008). *Strategies of Qualitative Inquiry, Handbook of Qualitative Research*, (3rd Edition), Britain: Sage Publigations.

Devlet Denetleme Kurulu (2013). Denetleme raporu. https://www.tccb.gov.tr/assets/dosya/ddk56.pdf. erişim: 13.10.2016.

Diker, A. & Varol, A. (2013). E-Ticaret ve güvenlik. *1. International Symposium on Digital Forensics and Security* , 29-33, Elazığ.

Doğan, M., & Morkoç, D. K. (2015). Seyahat acentalarının web sitelerini kullanma düzeyi: "Çanakkale 2015" teması üzerinden karşılaştırmalı bir analiz. *Batman Üniversitesi Yaşam Bilim Dergisi , 5 (2)*, 99-115.

Doğantimur, F. (2009). *ISO 27001 Standardı çerçevesinde kurumsal bilgi güvenliği* (Professional Qualification Thesis), TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara.

Eminağaoğlu, M. & Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , 11 (4)*, 1-15.

Erdoğan, G. & Bahtiyar, Ş. (2014). Sosyal ağlarda güvenlik. *M. Üniversitesi (Dü.), Akademik Bilişim'14 - XVI. Akademik Bilişim Konferansı Bildirileri içinde (s. 267-272).* Mersin: Mersin Üniversitesi.

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B. & Weippl, E. (2007). Information security fortification by ontological mapping of the ISO/IEC 27001 standard. In Dependable Computing, 2007. PRDC 2007. *13th Pacific Rim International Symposium on IEEE,* 381-388.

Ganbat, O. (2013). ''*Bilgi Güvenliği Yönetim Sistemi Iso/Iec 27001 ve Bilgi Güvenliği Risk Yönetimi Iso/Iec 27005 Standartlarının uygulanması*'', (Master Thesis), Ege Üniversitesi Fen Bilimleri Enstitüsü, İzmir.

Giritlioğlu, İ. (2014, Nisan). Türkiye'de yerel turizm ofislerinin web site içeriklerinin değerlendirilmesine yönelik bir araştırma. *KSÜ Sosyal Bilimler Dergisi , 11 (1)*, 89-102.

Grover, V. & Davenport, T. H. (2001). General perspectives on knowledge management: fostering a research agenda. *Journal of Management Information Systems , 18 (1),* 5-21.

Guan, B. C., Lo, C. C., Wang, P. & Hwang, J. S. (2003). Evaluation of information security related risks of an organization: the application of the multicriteria decision-making method. In Security Technology, 2003. *Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on IEEE,* 168-175.

Gürcan, İ. A. (2014). '' Assessing information security management requirements for finance sector using an ISO27001 based approach (Master Thesis), Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

Hekim, H. & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik Ve Terörizm Dergisi , 4 (2),* 135-158.

Henkoğlu, T. & Yılmaz, B. (2013). Avrupa Birliği (AB) bilgi güvenliği politikaları. *Türk Kütüphaneciliği Dergisi ,* 451-471.

Ho, C. I. & Lee, Y. L. (2007). The development of an e-travel service quality scale. *Tourism Management, 28(6),* 1434-1449.

İslamoğlu, H. (2009). *Sosyal Bilimlerde Araştırma Yöntemleri*. İzmit: Beta Yayınları.

http://www.hurriyet.com.tr/anonymous-emniyeti-hackledi-vatandasin-bilgileri-internete-dustu-40055371 erişim 20.03.2016.

Kara, M. (2013). ''*Siber saldırılar siber savaşlar ve etkileri*''. (PhD Thesis), İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Karadağ, E. (2010). Eğitim bilimleri doktora tezlerinde kullanılan araştırma modelleri: Nitelik düzeyleri ve analitik hata tipleri. *Kuram ve Uygulamada Eğitim Yönetimi, 16 (1),* 49-71.

Karamustafa, K. & Öz, M. (2010). Türkiye'de konaklama işletmelerinin web sitelerinde Yer verilen faktörlerin başarımı. *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 5(2),* 189-218.

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers ve Security, 25(4),* 289-296.

Kaya, U. (2015). DoxTracker: doküman kaçak takip sistemi (Master Thesis). İstanbul: Şehir üniversitesi, Fen Bilimleri Enstitüsü.

Liao, Z. & Shi, X. (2017). Web functionality, web content, information security and online tourism service continuance. *Journal of Retailing and Consumar Services, 39(2017),* 258-263.

Lin, SW & Fu, HP (2012). Seyahat acentelerinde müşteriden kişiye elektronik ticaret için kritik başarı faktörlerini ortaya çıkarmak. *Seyahat ve Turizm Pazarlaması Dergisi, 29 (6),* 566-584.

Lovrić, Z. (2012, September). Model of simplified implementation of PCI DSS by using ISO 27001 standard. *In proceedings of Central European Conference on Information and Intelligent System* , 347-351).

Marşap, A., Akalp, G., & Yeniman, E. (2010). Sağlık işletmelerinde insan kaynağının kurumsal bilgi güvenliği kültürü gelişimi. *International Journal Of Informatics Technologies, 3(1),* 31-40.

Mestçi, A. (2007). Türkiye internet raporu 2007. Beykent Üniversitesi Yönetim Bilişim Sistemleri Bölümü, *XII. "Türkiye'de İnternet" Konferansı,* Ankara.175-183.

http://www.milliyet.com.tr/hacklenen-emniyet-sitesinin-komik-sifresi-sektorel-1511863/ erişim 21.11.2016.

Sarıışık, M., & Akova, O. (2006). Seyahat acentalarında internetin rolü ve önemi. *Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , 12 (2),* 128-148.

Siber Güvenlik Derneği (2014). Siber güvenlik raporu. http://www.siberguvenlik.org.tr/ erişim 13.03.2016.

Susanto12, H., Almunawar, M. N. & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS, 11(5),* 23-29.

Tatar, N. (2015). ''The comparison of information security standards by using analytic hierarchy process''.(Master Thesis), Çankaya Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi,11(1),* 132-137.

Türker, A. & Türker, G. Ö. (2013, 01 30). Turistik ürün satın alma davranışının teknoloji kabul modeli ile incelenmesi. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi , 15 (2),* 281-312.

Üzümcü P. T. (2015). Otel yöneticilerinin turizm eğitimine yönelik algıları: Kocaeli ili otel yöneticileri üzerinde bir araştırma. *Kocaeli Üniversitesi Sosyal Bilimler Dergisi, (30),* 123-150.

http://www.udhb.gov.tr/images/duyurular/74bc0128f065b41.pdf erişim 23.11.2016.

Vural, Y. & Sağıroğlu, Ş. (2008, Şubat 18). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniv. Müh. Mim. Fak. Dergisi , 23 (2),* 507-522.

Yavanoğlu, U., Sağıroğlu, Ş. & Çolak, İ. (2012). Sosyal ağlarda bilgi güvenliği tehditleri ve alınması gereken önlemler. *Politeknik Dergisi , 15 (1),* 15-27.

Yayla, M. (2013). Hukuki Bir Terim Olarak "Siber Savaş". *TBB Dergisi, 104,* 194-198.

Yıldırım A. (1999). Nitel araştırma yöntemlerinin temel özellikleri ve eğitim araştırmalarındaki yeri ve önemi. *Eğitim ve Bilim Dergisi, 112 (23),* 1-11.

Yıldırım A. & Şimşek H. (2006). *Sosyal Bilimlerde Nitel Araştırma Yöntemleri.* (5th Edition) Ankara: Seçkin Yayınevi

Yıldız, S., & Yıldız, Z. (2015). Bilişim teknolojilerinin turizm pazarlaması, dağıtım sistemi ve seyahat acentelerinin iş modeli değişimine etkisi. *İnsan ve Toplum Bilimleri Araştırmaları Dergisi , 4 (3),* 595-611.

http://www.worldometers.info/tr/ erişim:28.02.2016.

http://www.tdk.gov.tr/index.php?option=com_bts&arama=kelime&guid=TDK.GTS.5b4c99413fdaa8.77819868 erişim: 16.08.2018

http://www.trtturk.com/haber/thy-hacklendi--8587.html erişim 17.03.2016.

http://www.mynet.com/haber/guncel/iett-hacklendi-2367277-1 erişim 30.03.2016.