GEOGRAPHY AND TOURISM, Vol. 10, No. 2 (2022), 7-15, Semi-Annual Journal
eISSN 2449-9706, ISSN 2353-4524, DOI: https://doi.org/10.34767/GAT.2022.10.06

Artur Kapera
AGH Univeristy of Science and Technology, Kraków, Poland, Apius Technologies S.A.
ORCID: https://orcid.org/0000-0002-5090-9197
Corresponding author: Artur Kapera, email: kaperaa@protonmail.com

Cybersecurity in travel based on the opinions of university students engaging in tourism

Abstract: Cybersecurity is a critical, yet often overlooked aspect of travelling domestically and abroad. Several issues connected with cybersecurity, such as the possibility of network-based attacks while connected to public wireless networks as well as matters connected with physical security of carried devices arise when travelling and are exacerbated with repeated border crossings or stays in several accommodation facilities. This study focuses on gauging the types of security precautions university students take when participating in tourism and providing recommendations based on the collected data and the responses taken from study participants. In the investigation, an analysis of source materials was used in conjunction with a diagnostic survey distributed among university students in Poland. In the study, the research hypothesis of "Among the surveyed students, most are at least partially security-conscious, but the majority fail to implement adequate measures of improving data confidentiality and availability on their personal devices while travelling" has been put forward.

Keywords: network security, tourism, cybercrime

1. Introduction

Since the start of the XXIst century, technology has permeated virtually every aspect of the tourism industry. In the United States, in 2019 98.5% of guests travelled with smartphones, and 65% of them connected to Wi-Fi within seven minutes of arrival at their destination accommodations (Hotel Internet Services, 2019). This shows that a large majority of tourists use Internet-connected devices connected to the Internet during travel and stay in hotels or other tourist accommodations. Along with the usage of electronic devices, cybersecurity issues, whose severity increases with how Internet-connected tourists' lives of tourists connected to the Internet. Thus, it is especially important to study the cybersecurity threats affecting university students, as they have been exposed to readily-available consumer electronics almost since birth, making them dependent on such technology for both their personal and professional lives (Prensky, 2001). It is especially important to study university students' cybersecurity habits while travelling for two significant reasons. First, there is a lack of scientific research from this angle at the time of writing of this document, and other studies concerning students' cybersecurity suggest that most students worldwide lack an understanding of the importance of cybersecurity (Sremath et al., 2016; Erendor, Yildirim, 2022; Garba et al., 2020).

The research proceedings included a review of source materials, followed by the preparation of a survey questionnaire aimed at students in Krakow. The author's own observations and experience in the cyber security industry were also helpful. The aim of the study was to present the main ways in which students ensure their IT security while engaging in tourism and to point out common mistakes or suggest improvements for the future.

2. Cybercrime

According to the European Commission, cybercrime can be defined as “criminal acts committed online by using electronic communications networks and information systems” (European Commission, https://home-affairs.ec.europa.eu/cybercrime_en). The Commission distinguishes between three broad types of cybercrime:

- Crimes specific to the Internet, such as attacks against information systems or phishing (e.g., fake bank websites to solicit passwords enabling access to victims’ bank accounts);
- Online fraud and forgery: large-scale fraud can be committed online through instruments such as identity theft, phishing, spam, and malicious code;
- Illegal online content, including child sexual abuse material, incitement to racial hatred, incitement to terrorist acts and glorification of violence, terrorism, racism and xenophobia” (European Commission, https://home-affairs.ec.europa.eu/cybercrime_en).

As of 2022, cybercrime is on the rise, and the trend does not show signs of slowing down. According to Cybersecurity Ventures, “global cybercrime costs [are expected] to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015” (Morgan, 2022). This worrying trend goes hand in hand with a generational one. According to a survey conducted by Savanta Inc. in 2021 in Germany, the US and the UK, the younger the survey participands, the less safe and private they feel on average while using the Internet (Malwarebytes, 2021). Among Savanta Inc.’s findings we can read that “only 26 percent of 18 – 34-year-olds [believe] their information is confidential online” (Malwarebytes, 2021). This begs the question of how such a steep rise in cybercrime costs impacts the tourism industry and whether young people, being so untrusting in online security, take appropriate precautions to limit information leakage.

3. Cybersecurity-related threats in the tourism industry

The tourism industry, being heavily dependent on electronic communication infrastructure, can expect cybersecurity-related issues to manifest themselves ever more noticeably, causing lost profits, dissatisfied customers, and potentially causing lasting damage, such as in the case of PII (Personally Identifiable Information) leaks. Among the most common methods of attacks against hotels and their customers is phishing. According to the IETF (Internet Engineering Task Force), phishing can be defined as “A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a Web site, in which the perpetrator masquerades as a legitimate business or reputable person” (Shirey, 2007). Phishing operations can be augmented with real booking data, extracted from sites such as Booking.com, to make fake e-mail messages more believable to unsuspecting customers (Whitehead, 2018). Travellers can protect against such attacks via conscientious checking of e-mail senders’ identities and verifying e-mails by making a phone call to the accommodation place, but there exist other types of phishing attacks that tourists cannot readily protect themselves against. Certain phishing campaigns are targeted directly at hotel staff (Gallagher, 2016), potentially causing the personal data of hundreds of unsuspecting guests to be leaked. The overall picture gets even more bleak, as Symantec has found that, from their analysis of more than 1500 hotels in 54 countries, “67% of hotel websites leak guests’ booking and personal details” to third parties, such as advertisers or analytics companies (Wueest, 2019). The details that were also leaked were not insignificant. According to Symantec’s research, “the majority [of hotel websites] leaked personal data, such as:

- Full name;
- Email address;
- Postal address;
- Mobile phone number;
- The last four digits of the credit card, the type of the card and expiration date;

– Passport number"(Wueest, 2019).

Phishing is not the only IT-related danger that can present itself to tourists. Hotel Wi-Fi networks are often not adequately secured and can be used by hackers to steal tourists' personal data and compromise travel devices. This can take the form of freelance hackers visiting hotels and trying to catch unprepared visitors or organised crime groups, some of them active for well over a decade, such as the notorious DarkHotel hacking group (Palmer, 2017), or the Russian APT28 group (Smith et al., 2017), both of which utilise public WiFi networks at hotels, public transport stations, and other locations, to spread malware. As such, it is extremely important for hotel guests to know about ways of protecting themselves from such attacks and simple ways of gauging the security of a public WiFi network (such as the usage of WPA 2/3, an industry standard for wireless network encryption).

Another danger facing certain travellers makes itself apparent at border crossings, especially in high-security locations like airports and international border crossings outside the EU. Under certain circumstances (varying from country to country), tourists may be requested by border crossing officials to present their digital devices, such as phones, laptops, and storage media, for inspection. Such searches are especially common for travellers crossing the United States, border, with 37 450 and 45 499 travellers having had their devices searched in 2021 and 2022, respectively (U.S. Customs and Border Protection, 2022). The practice has recently garnered even more controversy in the United States, with the release of information revealing that data (such as contacts, call logs, photos, and messages) garnered during such searches are being saved into a national database operated by the US Customs and Border Protection (Harwell, 2022). Moreover, The Washington Post reports that "2,700 CBP officers [can] access it without a warrant" (Harwell, 2022) putting travellers' data at even more risk. Travellers may have various reasons to want to avoid such practices. They range from a simple expectation of respect towards their privacy, to wanting to avoid possible incarceration for reasons of activism contrary to government interests, religious beliefs, ethnicity, or sexuality/gender expression. Under such circumstances, tourists need to know how to protect their devices. According to the Electronic Frontier Foundation, travellers should first and foremost 'decide whether they can reduce the amount of digital information they carry across the border' and 'use full disk encryption and backup their data elsewhere' (Schwartz et al., 2017). The EFF also points out that "travellers should not rely solely on fingerprint locks, which are less secure than passwords" (Schwartz et al., 2017).

4. Method and test sample

Empirical research was preceded by a literature review. The research process utilised a diagnostic survey method. In this research procedure, a diagnostic survey based on a questionnaire consisting of 29 questions was used. The survey was anonymous and was distributed among students of Polish universities, during a period spanning from July to September 2022. The survey involved 103 people, 25 of whom were women, 71 of which were men, and 7 of which refused to provide their gender. Statistical analysis was carried out on the research hypotheses:

H_1: University students taking cybersecurity take greater precautions than students taking other programmes when travelling.

H_2: Among the surveyed students, most are at least partially security conscious, but most fail to implement adequate measures to improve data confidentiality and availability on their personal devices while travelling.

To confirm or deny the research hypotheses, a scoring system based on the responses of the students survey was devised. Each answer (with exceptions such as partial question overlap and metrics) was assigned a positive or negative point value, depending on whether the answer indicated a positive or negative trend in individual IT-security-related protections. The point values were weighed to skew on the positive side (0 points were more commonly assigned for answers than negative values), but the minimum number of points possible to achieve was kept negative, to indicate detrimental security practices across the board.

The maximum number of points achievable was 23 and the minimum was -8.

5. Results

Only about 38% of respondents said that they always pay attention to IT security-related issues when travelling. 55% of respondents pay attention to such matters only occasionally, while 7% pay no attention at all (Figure 1).

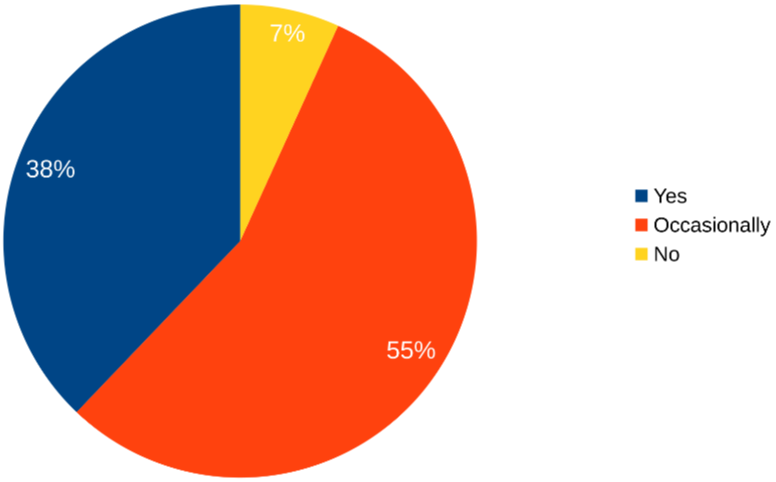

Figure 1. Attention given to cybersecurity by respondents when travelling (source: wn analysis based on questionnaire)

By far the most common security precautions taken by students while travelling are passwords, biometrics, such as fingerprints or face recognition and avoiding websites asking for personally identifiable information. The least commonly taken precautions include privacy filters on device displays, the usage of Tor and the conscious usage of device or file encryption (Figure 2). “Conscious” here was used deliberately, as Apple devices released after 2009 come pre-encrypted (Zinkus, et al., 2021),

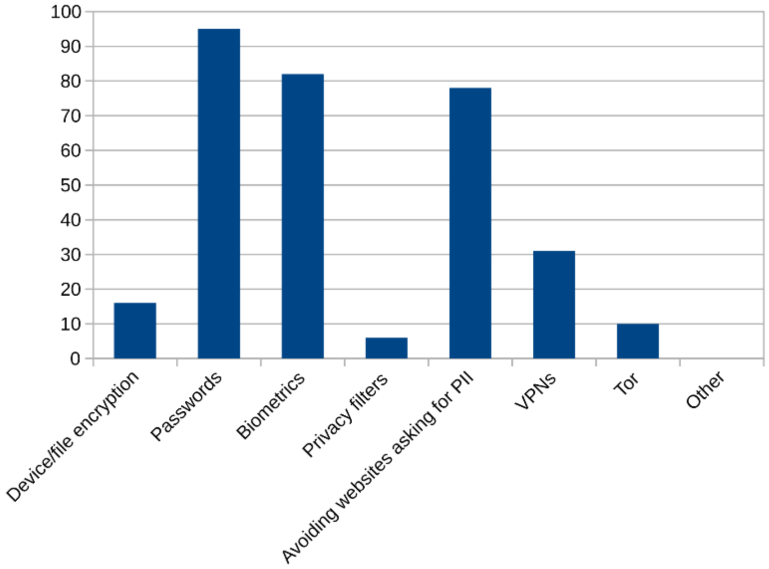

Figure 2. Types of IT security-related precautions taken by respondents (source: own analysis based on questionnaire)

as do most Android devices running Android 6.0 (released in late 2015) or later with Google Mobile Services certification (Raynor, 2021). This means that users will often make use of encrypted devices without knowing about the fact that they are encrypted.

The vast majority of respondents (71%) said that they use public WiFi networks at their places of accommodation. Interestingly, more respondents declared that they refuse to use public WiFi networks at all (28%) than use public WiFi at public transport stations, shopping malls, airports, etc. (26%) (Figure 3).

Of the 74 respondents that declared that they use public WiFi networks while travelling, only around half of them (51%) pay attention to the WiFi networks' security (whether they are "Open" networks or encrypted with protocols such as WPA2), while the rest (49%) do not.

Of the 103 respondents, most of them (93%) knew what a virtual private network was, while 71% have used VPN software before. Out of those, the three most popular reasons to use VPNs were the following.

– Security;
– Privacy protection;
– Bypassing region locks.

36% of respondents use VPN software to access company networks while travelling; this could be considered a potential security issue, if their devices are compromised through one of the plethora of ways discussed before that IT

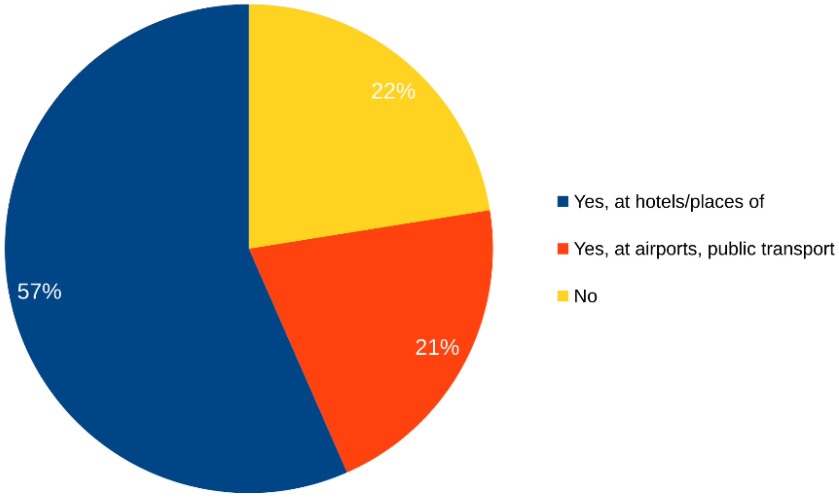

Figure 3. Respondents' willingness to use public WiFi networks while travelling (source: own analysis based on questionnaire)

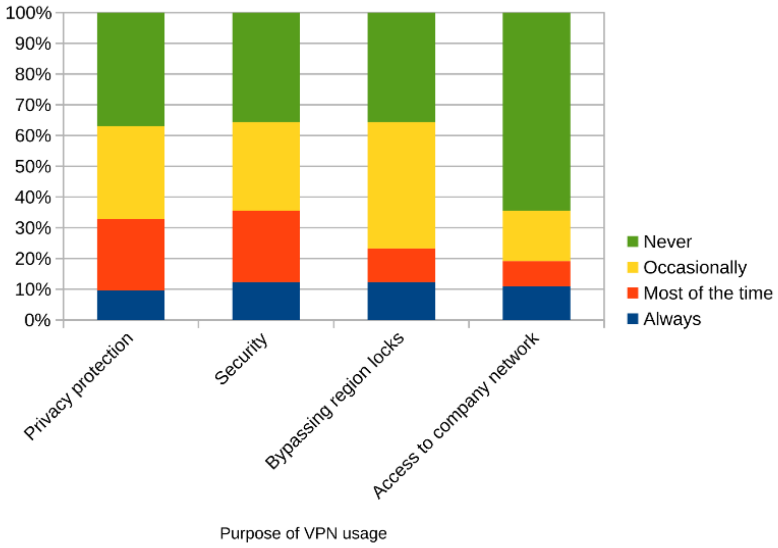

Figure 4. Respondents' usage of VPN technologies while travelling, grouped by purpose (source: own analysis based on questionnaire)

security can be bypassed. Of the 21% of respondents that use exclusively free of charge VPN software, a worryingly large fraction (32%) use them for reasons of improving privacy or security (Figure 4).

The scores achieved by survey participants ranged from 3 to 18 points, with the majority of the participants scoring between 1 and 11 (Figure 5). The average score attained was 5.4, with a standard deviation of 4.4 and a median of 4. Out of 103 participants, only seven managed to reach more than half of the available points. This means that 93% of participants do not take enough security precautions to achieve even half of the possible maximum score.

The average and median scores of participants are correlated with the university courses they attended (Figure 6). Participants taking cybersecurity-related courses scored 7 points on average with a median score of 7. Participants taking IT-related (but different from cybersecurity) courses scored on average 4.97 points with a median score of 4, and those taking courses unrelated to IT scored on average 4.23 points with a median score of 3.

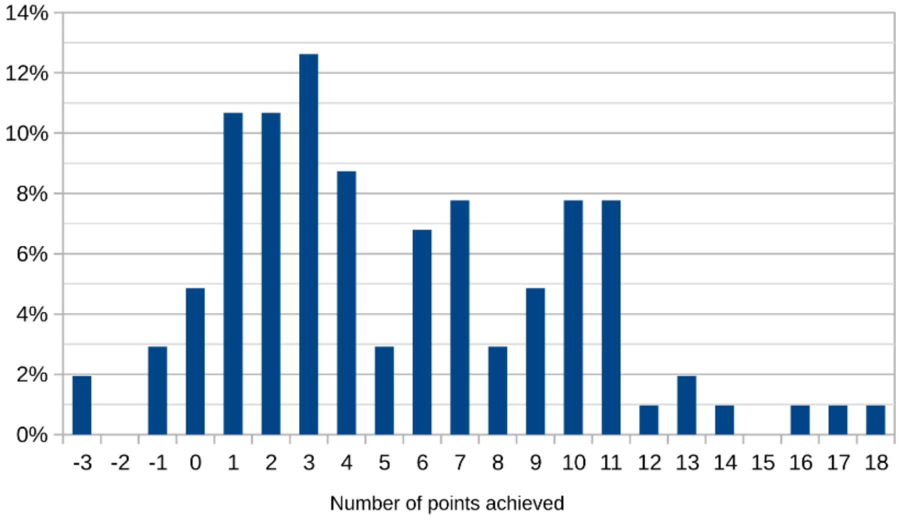

Figure 5. Distribution of scores of the participants, based on their responses to the survey (source: own analysis based on questionnaire)

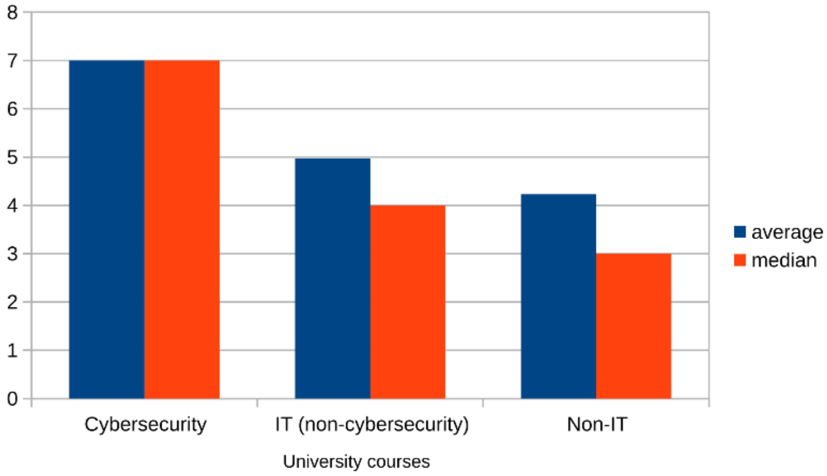

Figure 6. Average and median scores of participants, grouped by university courses attended (source: own analysis based on questionnaire)

6. Discussion

A strong, if unsurprising, correlation can be seen between the university courses taken and participants' scores. The highest scores attained are among students of cybersecurity-related courses, followed by IT-related courses and then the rest. This confirms Hypothesis 1. The difference between the cybersecurity and IT course scores is noticeably higher than the difference between the IT and other course scores. This could indicate that "general tech-savviness" attained from IT-related courses helps with being cybersecurity-conscious, but an explicit cybersecurity setting has an outsized influence on precautions taken. We also need to consider a possible selection bias: Students who were already security-conscious before deciding to attend university may have had a preference for attending cybersecurity-related courses. Thus, while the relationship between attending cybersecurity-related courses and score is correlational, further research is needed to decide whether it is causal and by how much. With the extremely large amount of possible cybersecurity threats students may encounter while travelling and the fact that each of these may require a separate precautionary step to be taken, it is not surprising that none of the surveyed students managed to achieve the maximum score available. However, it is worrying that an overwhelming majority of participants (93%) didn't manage to attain even half of the available points. This shows that most of the students surveyed students do not take nearly enough cybersecurity-related precautions while travelling, confirming Hypothesis 2.

A worrying statistic from the point of view of security and privacy is the fact that 32% of respondents that declared the exclusive usage of free of charge VPN software used it for reasons of increasing their online security or privacy while travelling. This could stem from a fundamental misunderstanding of the business model of such services. They are 'free of charge' only because they profit from the personal data of their users, many of which can be revealed through the analysis of user browsing habits (Orphanides, 2020). Certain VPN applications do not stop at a simple analysis of traffic — some go as far as manipulating the traffic itself, from inserting advertisements into unencrypted websites, scanning the device they are installed on for all marketable information, and even TLS interception, which is an enormous security issue that could result in sensitive credentials (such as bank passwords) being stolen/ leaked (Ikram et al., 2016). Despite having lived most of their lives around Internet-connected devices (Prensky, 2001), most surveyed students show worryingly little regard for cybersecurity online. Global cybercrime is not predicted to go down in the near future (Morgan, 2022).

7. Conclusions

The analysis shows that much more effort needs to be put into cybersecurity education, and from as young an age as possible. This should be a two-fold approach; first of all, students should be made aware of the possible dangers they can expect to face in an always online world and why it's extremely important for them to focus on protecting themselves. Even if you do not plan to work "in IT", it is very possible that most of your work will involve interfacing with a computer system. Thus, inadequate precautions can cause enormous damage. Secondly, students need to be taught practical, specific ways of protecting themselves, with each method presented in detail and with exemplary pieces of software being presented. Students also need to be made aware that engaging in tourism expands the possible cybersecurity-related threats they may face considerably. Furthermore, such educational measures should not stop at students - companies and organisations providing tourist services also need to teach their employees proper ways to engage with cyber threats.

Limitations

It is proposed that future research should cover a broader sample of respondents, including also include international students, as access to modern technology and attitudes toward cybersecurity may vary from country to country. In addition, it is also desirable to examine other correlations, such as those related to the distance travelled.

References

Erendor M.E., Yildirim M., 2022. Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access 10, 52319-52335, DOI: 10.1109/ACCESS.2022.3171829.

Garba A., Siraj M., Alhaji Musa M., Othman S., 2020. A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach. International Journal on Emerging Technologies 11(5), 41-49.

Ikram M., Vallina-Rodriguez N., Seneviratne S., Kaafar M.A., Paxson V. 2016. An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps. [In] Gill P., Heidemann J. [Eds.] Book of Proceedings IMC 2016: Internet Measurement Conference, November 14-16, Santa Monica, California, USA, 349–364, https://doi.org/10.1145/2987443.2987471.

Prensky M., 2001. *Digital Natives, Digital Immigrants*. On the Horizon 9(5), 1-6, DOI:10.1108/10748120110424816.

Shirey R.W., 2007. Internet Security Glossary, Version 2. Request for Comments (RFC) 4949. Copyright Internet Engineering Task Force (IETF), 364, DOI: https://doi.org/10.17487/RFC4949.

Sremath Tirumala S., Sarrafzadeh A., Pang P., 2016. A survey on internet usage and cybersecurity awareness in students. [In:]Sarrafzadeh M. [Ed.] Book of Proceedings 14th Annual Conference on Privacy, Security and Trust (PST), 12-14 December, Auckland, New Zeland, DOI: https://doi.org/10.1109/ PST.2016.7906931.

Zinkus, M., Jois, T.M., Green, M. 2021. Data security on mobile devices: Current state of the art, open problems, and proposed solutions. arXiv, 118, https://arxiv.org/pdf/2105.12613.pdf.

Internet sources

European Commission, Cybercrime, https://home-affairs.ec.europa.eu/cybercrime_en (Date of access: 01.11.2022).

Gallagher S., 2016. Checking in with spear phishing, criminals check out with hotel credit card data, https://arstechnica.com/information-technology/2016/05/hotels-face-increasingly-targeted-attacks-on-customer-data/ (Date of access: 27.09.2022).

Harwell D., 2022. Customs officials have copied Americans' phone data at massive scale. Washington Post, https://www.washingtonpost.com/technology/2022/09/15/government-surveillance-database-dhs/ (Date of access: 27.09.2022).

Hotel Internet Services, 2019. Meeting Hotel Guest Wi-Fi Expectations in the Age of Hyper Connectivity and IoT. Hotel Internet Services, https://www.hotelwifi.com/wp-content/uploads/2019/02/WiFi_Whitepaper.pdf (Date of access: 27.09.2022).

Malwarebytes Inc., Demographics of Cybercrime Report, https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html#younger (Date of access: 27.09.2022).

Morgan S., 2022. Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics. Cybercrime Magazine, https://cybersecurityventures.com/cybersecurity-almanac-2019/ (Date of access: 27.09.2022).

Orphanides K.G, 2020. Free VPNs are a privacy nightmare. You shouldn't download them. Wired UK, https://www.wired.co.uk/article/free-vpn-android-ios-privacy (Date of access: 27.09.2022).

Palmer D., Hackers are using hotel Wi-Fi to spy on guests, steal data. ZDNET, https://www.zdnet.com/article/hackers-are-using-hotel-wi-fi-to-spy-on-guests-steal-data/ (Date of access: 27.09.2022).

Raynor E., 2021. Everything you need to know about Android encryption. Hexnode Blogs, https://www.hexnode.com/blogs/everything-you-need-to-know-about-android-encryption/ (Date of access: 27.09.2022).

Schwartz A., Sophia C., Kalia A., Schoen S., 2017. Digital Privacy at the U.S. Border: Protecting the Data On Your Devices, https://www.eff.org/wp/digital-privacy-us-border-2017 (Date of access: 27.09.2022).

Smith L., Read B., 2017. APT28 Targets Hospitality Sector, Presents Threat to Travelers, https://www.mandiant.com/resources/blog/apt28-targets-hospitality-sector-presents-threat-travelers (Date of access: 27.09.2022).

U.S. Customs and Border Protection, CBP Enforcement Statistics Fiscal Year 2022, https://www.cbp.gov/newsroom/stats/cbp-enforcement-statistics (Date of access: 27.09.2022).

Whitehead J., 2018. *Booking.com targeted by hackers with email scam asking customers for payment details*, https://www.independent.co.uk/travel/news-and-advice/travel-website-hackers-cyber-crime-phishing-holidays-a8382771.html (Date of access: 27.09.2022).

Wueest C., 2019. Two in Three Hotel Websites Leak Guest Booking Details and Allow Access to Personal Data, http://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hotel-websites-leak-guest-data (Date of access: 27.09.2022)