Fraud Detection in E-Commerce

Sara Alqethami[1], Badriah Almutanni[2] and Manal AlGhamdi[3]
maalghamdi@uqu.edu.sa
College of Computer Science and Information System, Umm Al-Qura University, Makkah, Saudi Arabia

Abstract
Lack of knowledge and digital skills is a threat to the information security of the state and society, so the formation and development of organizational culture of information security is extremely important to manage this threat. The purpose of the article is to assess the state of information security of the state and society. The research methodology is based on a quantitative statistical analysis of the information security culture according to the EU-27 2019. The theoretical basis of the study is the theory of defense motivation (PMT), which involves predicting the individual negative consequences of certain events and the desire to minimize them, which determines the motive for protection. The results show the passive behavior of EU citizens in ensuring information security, which is confirmed by the low level of participation in trainings for the development of digital skills and mastery of basic or above basic overall digital skills 56% of the EU population with a deviation of 16%. High risks to information security in the context of damage to information assets, including software and databases, have been identified. Passive behavior of the population also involves the use of standard identification procedures when using the Internet (login, password, SMS). At the same time, 69% of EU citizens are aware of methods of tracking Internet activity and access control capabilities (denial of permission to use personal data, access to geographical location, profile or content on social networking sites or shared online storage, site security checks). Phishing and illegal acquisition of personal data are the biggest threats to EU citizens. It have been identified problems related to information security: restrictions on the purchase of products, Internet banking, provision of personal information, communication, etc. The practical value of this research is the possibility of applying the results in the development of programs of education, training and public awareness of security issues.
Keywords: *Information Security, Digital Skills, Information Space, Security Culture, Data Protection.*

1. Introduction

One of the catalysts of globalization in post-industrial society is the growing informatization of human civilization and the gradual, stable entry of national information spaces of individual states into the European and world information sphere. This space, the main components of which are information resources, means of information interaction, and information infrastructure, is a sphere of modern social life in which information communications play a leading role. Unfortunately, this sphere of human life and society has not gone unnoticed by the subversive activities of special services of foreign states, criminals (in particular, extremists and terrorists), whose activities are gradually becoming transnational in nature. Therefore, there is a problem of protection of information space as one of the components of security of the state and society. Ensuring the information security of the state and society depends on the synergy of resources of the private and public sectors, in particular the responsibility and knowledge of citizens about the rules of conduct in the information space and ways to protect personal data, information assets. Certain political forces use crisis phenomena of a social nature and the situation around them systematically, to satisfy their own political ambitions and to form a negative informational influence. This kind of ideological struggle or information war sometimes has more catastrophic consequences than physical violence, terrorist attacks, or murders. Modern information terrorism is a kind of technology of interfering in social processes, when by provoking mass terrorophobia, distrust, hatred, and open hostility, they try to change or adjust the algorithm of social management, to replace the natural development of social processes and systems in favor of their own political views. Unfortunately, the world community has so far failed to develop optimal counter-terrorism strategies, limiting itself to continuous improvement in the fight against terrorism and its consequences. Lack of knowledge and digital skills is a threat to information security of the state and society, so the formation and development of organizational culture of information security is extremely important for managing this threat (AlHogail & Mirza, 2014). Due to the low level of awareness in the field of information security, the following types of threats may arise: damage to information assets, fraudulent transactions, illegal dissemination of personal data for commercial purposes, psychological pressure (discrimination, harassment, bullying). Therefore, the culture of information security is a prerequisite for protection and elimination of potential threats and risks. The culture is also a prerequisite for the behavior of citizens in the information space, as "in information security the human element consider the most of weakest link in general" (Mahfuth, 2017). To address the problems related to the "human factor", it is proposed to develop a culture of information security aimed at human behavior so that information security becomes part of the beliefs of society (Okere, 2012).

The purpose of the article is to assess the state of information security of the state and society.
To achieve this goal, the following tasks are defined:
1. Assess the ways and level of development of digital skills of citizens within the EU.
2. Assess the risks of information security threats and the extent of possible losses.
3. Assess the ways of protection in the information space and the behavior of EU citizens.
4. Assess the level of awareness (culture) of information security and protection of citizens.
5. Assess problems in the field of information security.

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.40

6. Assess the problems of restricting activities on the Internet through technical protection tools.

2. Literature review

The issues of information security culture and information terrorism are actively discussed in the scientific literature. In their publications, scientists claim that the modern information space has finally become one of the main areas of political, economic, ethno-confessional struggle and is also used by terrorist organizations. Actions in the media sphere allow to cause significant damage to the object of attack without physical intervention, but only by imposing the necessary meanings and narratives. The need to impose one's will through direct violence has disappeared, giving way to information terrorism, which requires society to take new approaches in the field of law, change standards and approaches to the exchange of information and its dissemination (Varenia, Avramenko, 2020).

Van Niekerk & Von Solms (2010) consider the concept of corporate culture, according to which the knowledge and awareness of staff determines the level of security. Information security awareness is an individual's knowledge of particular security threats and the potential countermeasures against those threats" (Hanus & Wu, 2016). To disseminate a sufficient level of knowledge about protection in the information space and threats, international standards such as ISO/IEC 27002 (International Standards Organization, 2005) recommend the implementation of an information security awareness campaign. Behavior in the information space depends on the information culture of the individual in society (Da Veiga & Eloff, 2010): a higher level of culture ensures the reduction of risks and threats to state security, effective management of individual behavior when interacting with information assets (AlHogail, 2015). Lebek et al. (2014) identify four main theories of behavior: planned behavior theory (TPB), general deterrence theory (GDT), protection motivation theory (PMT), and technology acceptance model (TAM). PMT determines awareness of the determinant of an individual's behavior with information assets (Hanus & Wu, 2016). Therefore, it is important to monitor the level of awareness and culture in society. The human factor (Da Veiga & Martins, 2015) plays an important role in shaping the culture of information security, in particular the readiness of society, responsibility, governance, rules in society (AlHogail, 2015). Companies are responsible for raising the culture of information security and familiarizing staff with the policy. This minimizes human risks, incidents and staff errors by ensuring more responsible citizen behavior (Da Veiga, 2016). Creating a positive information security culture (ISC) is an effective mechanism for promoting behavior and security practices among citizens (Nasir, 2019). Knowledge of information policies and protection procedures, attitudes toward policies and procedures, and the behavior of every citizen can increase cybersecurity (Parsons, 2015).

A review of the scientific literature indicates the lack of a comprehensive study of information security. As noted by Karlsson, Åström & Karlsson (2015), much research is descriptive, philosophical or theoretical, and there is a lack of structured use of empirical data in the literature.

3. Methodology

Research concept (theoretical background)

This study used the theory of defense motivation to assess the level of awareness and knowledge of society in the field of information security (Hanus & Wu, 2016). Protection Motivation Theory (PMT) involves a person predicting the negative consequences of certain events and the desire to minimize them, which determines the motive for protection. In general, PMT includes two processes - threat assessment and coping assessment, which are used to explain individual behavior. Threat assessment consists of imaginary vulnerability (PV) and imaginary severity (PS). The first element of PV is the probability of a negative event, while the second element of PS is the size of the potential consequence if a negative event occurs. Overcoming scores include response efficiency (RE), SE and response cost (RC). RE can be defined as the confidence that

Model

The study developed a conceptual model of protection motivation based on PMT theory and EU data on the level of awareness of threats, the level of digital skills of citizens of EU member states, the level of current costs for replacing fixed information assets in all areas of activity in case of threat. The developed conceptual model was tested based on data on information security, information risks and threats.

PV (probability of occurrence of a negative event) is estimated on the basis of data on Security related problems experienced when using the internet for 2019, Privacy and protection of personal data (2020 onwards).

PS (size of potential impact) is estimated based on Eurostat data on current costs for the replacement of fixed information assets in all areas of activity for 2019 in the event of information threats. Information assets include ICT equipment (net), Computer hardware (net), Telecommunications equipment (net), Computer software and databases (net).

RE (indicator of minimizing the risks of negative events by the individual in the information space) is assessed based on indicators: 1. Activities via internet not done because of security concerns for 2019 (indicator that characterizes the passive role of the individual in overcoming information security risks). 2. Individuals' level of digital skills 2019, Way of obtaining ICT skills 2019, 3. Privacy and protection of personal data (2020 onwards) (indicators that characterize the active behavior of the individual in overcoming the risks of information security).

RC (the indicator of the volume of a fixed asset, which because of effective behavior of the individual in the event of a threat, was preserved) is based on the volume of current costs to replace fixed information assets in all areas of activity in 2019 in case of information threats.

4. Results

Digital skills determine the potential of society to ensure its own information security. Within the EU, 29% of the population has a low level of digital skills with a significant level of differentiation by country (deviation 10,277) (Table 1). Basic general digital skills are present in 25% of the population with a deviation of 5.413%, a high level of digital skills is available in 31% of the population and 56% are characterized by basic or above basic overall digital skills with a deviation within countries of 16.926%.

Table 1. Individuals' level of digital skills in the EU-27 in 2019

	EU-27	Standard deviation
Individuals who have low overall digital skills	29	10,277
Individuals who have basic overall digital skills	25	5,413
Individuals who have above basic overall digital skills	31	13,582
Individuals who have basic or above basic overall digital skills	56	16,926
Individuals who have no overall digital skills	1	0.898

Source: Eurostat (2021a).

EU society is characterized by the participation of citizens in free trainings or independent classes to improve the skills of using computers, applications or software (10% with a deviation of 8,249). The level of citizen participation in paid trainings for digital skills development is low (2% with a deviation of 2,527). The share of individuals who participated in trainings commissioned by the state or organizations was 3% within the EU with a differentiation of 2.541%, which indicates a low level of state funding to increase digital skills and awareness in the field of information security culture.

For comparison, the share of citizens in training to raise digital awareness at the expense of the private sector was 8% with a deviation of 6.985%. The share of persons trained during production was 10% with a deviation of 8.853% (Table 2). Thus, the behavior of the individual to overcome threats in the field of information security is passive; the main actor in ensuring the protection of information assets and minimizing risks is the private sector, which funds training in the development of digital skills. The question arises about the effectiveness of free digital skills training.

Table 2. Way of obtaining ICT skills in the EU-27 in 2019

	EU-27	Standard deviation
Individuals carried out free online training or self-study to improve skills relating to the use of computers, software or applications	10	8,249
Individuals carried out training paid by themselves to improve skills relating to the use of computers, software or applications	2	2,527
Individuals carried out free training provided by public programs or organizations to improve skills relating to the use of computers, software or applications	3	2,541
Individuals carried out training paid or provided by the employer to improve skills relating to the use of computers, software or applications	8	6,985
Individuals carried out on-the-job training to improve skills relating to the use of computers, software or applications	10	8,853

Source: Eurostat (2021b).

The current cost of replacing the total amount of fixed assets (net) in all activities is 43,009,117.6 million euros in 2019, of which the largest cost is to replace in case of damage Computer software, databases, ICT equipment, Telecommunications equipment (net), and Computer hardware (net). Thus, the most vulnerable are databases and software, the replacement cost of which in case of damage will be the largest amount.

Table 3. Current replacement costs of total fixed assets (net) in all NACE activities in EU-27 2019, million euros

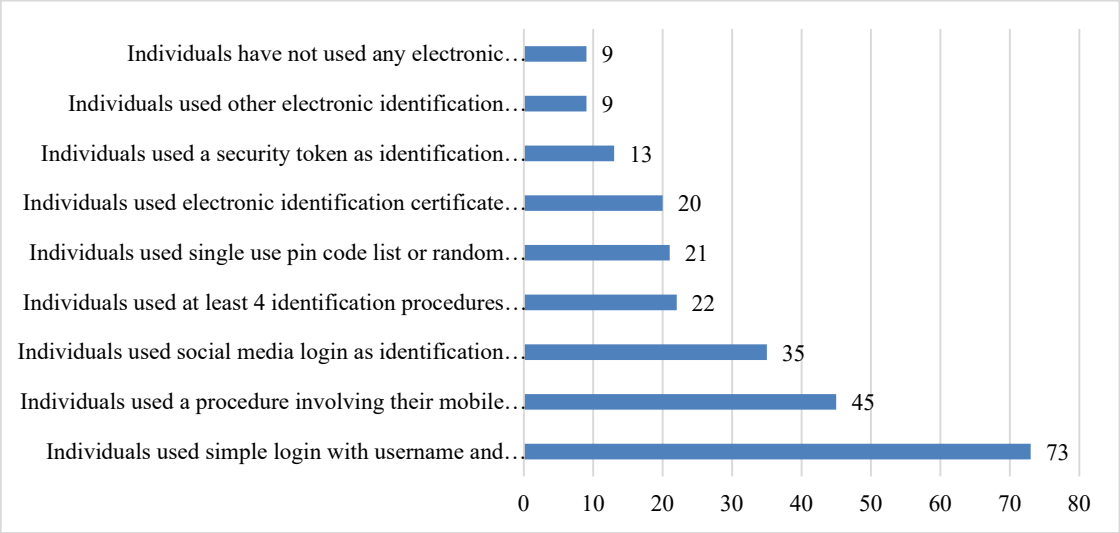
	Total, million euros in the EU-27	Average, million euros	Standard deviation, million euros
Total fixed assets (net)	43009117.60	1792046,57	2806336.60
ICT equipment (net)	369558.20	16798.10	22169.99
Computer hardware (net)	180429,90	7844.78	10689.24
Telecommunications equipment (net)	189354.00	8607.00	12199.74
Computer software and databases (net)	623631.50	28346.89	51137.88

Source: Eurostat (2021c).

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.40

To protect data and ensure information security, EU citizens mainly use a simple login with a username and password as an identification procedure to access online services (73%). 43% use a code sent via SMS to identify and access Internet services. 35% of citizens use login on social networks to identify and access services. 22% of citizens use at least 4 identification procedures to access the Internet. 21% of citizens use a one-time list of PIN codes or random password characters as an identification procedure to access Internet services. 20% of citizens used an electronic identification certificate or a card with a card reader or a program as an identification procedure to access online services. 13% of people used a security token as an identification procedure. 9% of people use other electronic identification procedures, 9% do not use any electronic identification procedure (Figure 1).

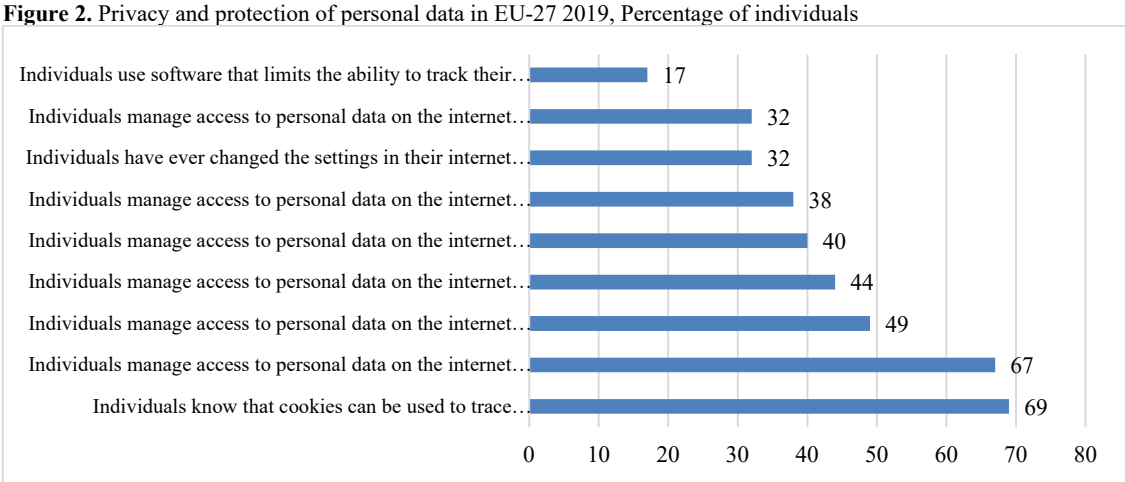
Figure 1. Identification procedures used for online services in EU-27 in 2019, Percentage of individuals



Source: Eurostat (2021d).

The protection of personal data depends on the awareness of privacy among citizens and the tools to ensure it. As a result, 69% of EU citizens are aware of the possibility of using cookies to track a person's movement on the Internet (activity tracking). 67% of citizens are aware that they can control access to personal data on the Internet. 49% of citizens control access to personal data on the Internet and have refused to allow the use of personal data for advertising purposes. 44% of people restricted or denied access to their geographical location. 40% of citizens read the privacy statements before providing personal data. 38% of people have restricted access to a profile or content on social networking sites or shared online storage. 32% of citizens changed their Internet browser settings to prevent or restrict cookies on any of their devices. 32% of people checked whether the website to which personal data was provided was secure. 17% of people use software to limit the ability to track their activities on the Internet (Figure 2).

Figure 2. Privacy and protection of personal data in EU-27 2019, Percentage of individuals

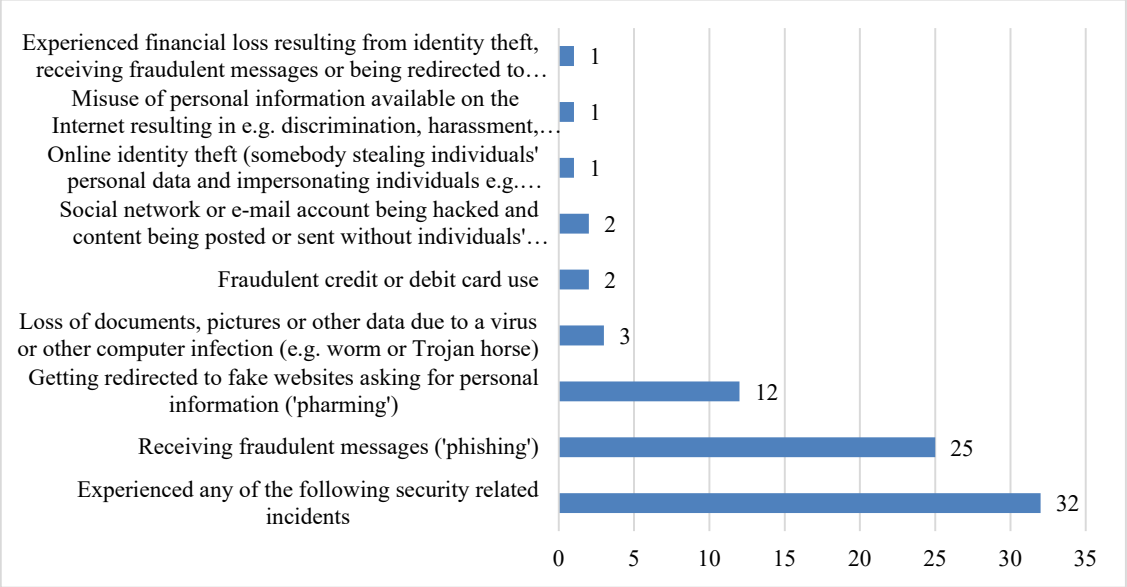


Source: Eurostat (2021e).

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.40

When using the Internet there are security problems, including: 32% of people have phishing - incidents related to receiving fraudulent messages; in 25% - redirection to fake websites with a request to provide personal information; 12% lost documents, images or other data due to a virus or other computer infection; 3% encountered fraudulent use of a credit or debit card; 2% have experienced a hacking of a social network or email account, posting or sending content posted without the knowledge of people; 2% encountered the theft of personal data on the Internet (for example, making a purchase under the name of a person); 1% of citizens have faced abuse of personal information available on the Internet, which leads to discrimination, harassment, bullying; 1% of people reported financial losses caused by identity theft, receiving fraudulent messages or redirecting to fake websites (Figure 3).

Figure 3. Security related problems experienced when using the internet in EU-27 in 2019, Percentage of individuals



Source: Eurostat (2021f).

At the same time, security causes restrictions on the activities and operations of individuals on the Internet. For example, security issues restrict or prevent people from ordering or buying goods or services (16%), providing services through banking (14%), providing personal information to social or professional network services (25%), communicating with government services or administrations (8%), download software or programs, music, video files, games or other data files (17%), use the Internet via public Wi-Fi (18%), other activities (7%) (Table 3).

Table 3. Activities via internet not done because of security concerns in EU-27 2019, Percentage of individuals

	EU-27	Standard deviation
Security concerns limited or prevented individuals from ordering or buying goods or services	16	7,255
Security concerns limited or prevented individuals from carrying out internet banking	14	5,515
Security concerns limited or prevented individuals from providing personal information to social or professional networking services	25	12,096
Security concerns limited or prevented individuals from communicating with public services or administrations	8	4,269
Security concerns limited or prevented individuals from downloading software or apps, music, video files, games or other data files	17	9,050
Security concerns limited or prevented individuals from using the Internet via public Wi-Fi	18	8,872
Security concerns limited or prevented individuals from doing other activities	7	13,802

Source: Eurostat (2021).

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.40

Thus, the study shows that the theory of motivation to protect in practice in the field of information security has virtually no manifestations. Passive behavior of individuals on the Internet does not involve predicting the negative consequences of certain events and the desire to minimize them, which leads to a lack of motivation to defend. The majority of the population uses standard protection procedures offered by private software developers. It is obvious that the motive for protection is more typical for persons who have faced threats to their own information security and use more reliable protection procedures. Individuals can hardly assess the threats and ways to overcome them until the problem situation arises. This may be due to a low level of awareness of possible threats and risks. The development of digital skills in this case does not provide overcoming the negative consequences of threats, until the person is aware of the full range of risks in the information space. Individuals also underestimate the magnitude of the potential consequences. Passive behavior of individuals maximizes the risks of negative events in the information space. Therefore, information security policy should be aimed at developing information campaigns to inform about potential threats, ways to overcome them and possible losses.

5. Discussion

Modern terrorist activity is based on the latest hybrid social information technologies for manipulating human consciousness, the systemic elements of which have long been hostage-taking, arson, murder, torture, intimidation of the population and the authorities. Terrorism in a post-industrial society has mastered innovative mechanisms for committing criminal encroachments not so much on people's lives or health as on their thoughts, morals, and spirituality.

Organizations recognize staff as the weakest link in information security. On the other hand, human resources are assets to reduce risks, if digital skills development is funded (Bulgurcu, Cavusoglu & Benbasat, 2010). According to this study, organizations are most interested in staff training in digital skills development, while citizens themselves are less active in the development of digital competencies. Since employees who adhere to the rules and norms of information security of the organization are the key to strengthening information security, employees' understanding of behavior in the information space of compliance is crucial for organizations that use human capital (Bulgurcu, Cavusoglu & Benbasat, 2010). According to the theory of planned behavior, Citizens' beliefs about compliance with information security rules depend on the benefits they receive, the cost of compliance, and the cost of non-compliance (Bulgurcu, Cavusoglu & Benbasat, 2010). This study found that citizens could not independently assess the losses due to risks in the information space. This means that a person's beliefs require external intervention: from the organization or the state. Therefore, the implementation of information campaigns on potential threats and losses because of security problems is relevant in this case.

Despite the technological security in the information space, there are a number of threats faced by users, including phishing and illegal data acquisition. This confirms the view of Tang & Zhang (2016) that information security cannot rely solely on technology. More attention needs to be paid to the behavioral aspects of users in the field of information security. Culture should encourage employees to follow information policies related to the collection, storage, dissemination and management of information.

Manuscript received June 5, 2021
Manuscript revised June 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.6.40

6. Conclusion

Given the political situation in the world, information terrorism, which includes cyberterrorism and media terrorism, has become relevant. Insufficient attention to this area greatly facilitates the implementation of cyber threats and therefore requires information, personnel, scientific, organizational, legal, psychological support in the context of anti-terrorist security. For example, the existing threats to information security can be identified through the negative, but currently not illegal, information impact on the consciousness and behavior of citizens, as well as through the impact on information resources and information technology infrastructure. Effective counteraction to such threats can be achieved only through the application of integrated approaches to the definition of "information security", "information terrorism", and countering fakes should become an element of state information security policy. This study found passive behavior of EU citizens in ensuring information security, which is confirmed by the low level of participation in trainings for the development of digital skills and mastery of basic or above basic overall digital skills 56% of the EU population with a deviation of 16%. High risks to information security in the context of damage to information assets, including software and databases, have been identified. Passive behavior of the population also involves the use of standard identification procedures when using the Internet (login, password, SMS). At the same time, 69% of EU citizens are aware of the methods of tracking Internet activity and access control capabilities (refusal to allow the use of personal data, access to geographical location, to a profile or content on social networking sites or shared online storage, site security checks). Phishing and illegal acquisition of personal data are the biggest threats to EU citizens; identified problems related to information security: restrictions on the purchase of products, Internet banking, provision of personal information, communication, etc.
Further research should be aimed at identifying ways to implement information campaigns within the EU to inform citizens about potential threats, ways to overcome them and possible losses.

References

[1] AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575.
[2] AlHogail, A., & Mirza, A. (2014, January). Information security culture: a definition and a literature review. In *2014 World Congress on Computer Applications and Information Systems (WCCAIS)* (pp. 1-7). IEEE.
[3] Alnatheer, M. A. (2015, April). Information security culture critical success factors. In *2015 12th International Conference on Information Technology-New Generations* (pp. 731-735). IEEE.
[4] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.
[5] Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19.
[6] Da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security

policy and those who had not: Illustrated through an empirical study. *Information & Computer Security*.
[7] Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security*, *29*(2), 196-207.
[8] Da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, *49*, 162-176.
[9] El-kenawy, E. S. M. T., Saber, M., & Arnous, R. (2019). An Integrated Framework to Ensure Information Security Over the Internet. *International Journal of Computer Applications*, *975*, 8887.
[10] Eurostat (2021a). Individuals' level of digital skills. https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_sk_dskl_i&lang=en
[11] Eurostat (2021b). Way of obtaining ICT skills. https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_sk_how_i&lang=en
[12] Eurostat (2021c). Cross-classification of fixed assets by industry and by asset (stocks). https://ec.europa.eu/eurostat/web/main/data/database?p_p_id=NavTreeportletprod_WAR_NavTreeportletprod_INSTANCE_nPqeVbPXRmWQ&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view
[13] Eurostat (2021d). Identification procedures used for online services (2020 onwards). https://appsso.eurostat.ec.europa.eu/nui/setupDownloads.do
[14] Eurostat (2021e). Privacy and protection of personal data (2020 onwards). https://appsso.eurostat.ec.europa.eu/nui/setupDownloads.do
[15] Eurostat (2021f). Security related problems experienced when using the internet. https://appsso.eurostat.ec.europa.eu/nui/setupDownloads.do
[16] Eurostat (2021g). Activities via internet not done because of security concerns. https://appsso.eurostat.ec.europa.eu/nui/setupDownloads.do
[17] Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, *33*(1), 2-16. https://doi.org/10.1080/10580530.2015.1117842
[18] Karlsson, F., Åström, J., & Karlsson, M. (2015). Information security culture–state-of-the-art review between 2000 and 2013. *Information & Computer Security*.
[19] Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*. 37 (12), 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085
[20] Mahfuth, A., Yussof, S., Baker, A. A., & Ali, N. A. (2017, July). A systematic literature review: Information security culture. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
[21] Nasir, A., Arshah, R. A., Ab Hamid, M. R., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12-22.
[22] Okere, I., Van Niekerk, J., & Carroll, M. (2012, August). Assessing information security culture: A critical analysis of current approaches. In *2012 Information Security for South Africa* (pp. 1-8). IEEE.
[23] Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.
[24] Tang, M., & Zhang, T. (2016). The impacts of organizational culture on information security culture: a case study. *Information Technology and Management*, *17*(2), 179-186.
[25] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers & security*, *29*(4), 476-486.
[26] Varenia N., Avramenko S. (2020) Virtual reality as a new global factor for analyzing the level of terrorist threat. *Ukrainian Journal of International Law*, 2, 46–60. https://doi.org/10.36952/uail.2020.2.46-60