SAFETY&DEFENSE
ISSN 2450-551X

The Analysis of Behavior of Internet Users from the Perspective of Their Safety

Tomasz STEFANIUK[1]

[1] University of Natural Sciences and Humanities, Siedlce, Poland;
tstefaniuk@uph.edu.pl, ORCID: 0000-0001-5769-8735

DOI: https://doi.org/10.37105/sd.62

Abstract

The Internet has become a ubiquitous medium that absorbs a greater proportion of our time. In addition to its unquestionable advantages, it presents a number of threats to the security of its users. The aim of the article is to analyze the ways in which individuals in different countries use the Internet and to examine the security implications resulting from the increasing popularity of the medium. The study presents the results of research conducted in the years 2018-2019 on a group of 562 Internet users from three countries: Spain, Poland and Turkey. The analysis of the results creates a gloomy picture of network users, who - despite risk awareness - do little to defend themselves against the threats until personally affected.

Keywords: behavior of Internet Users, Internet Users safety, risks relating to Internet use, safety.

1. Introduction

The Internet is one of the basic sources of information and tools of communication. Nowadays, the majority of people in developed and developing countries has Internet access. According to the "Digital 2019" Report, 360 million new Internet users appeared in the year 2018. This translates into 11 new users per second, i.e. an average of one million new users every day. At present, 4.388 billion people, i.e. 57% of the global population is online. This constitutes a growth of 9% with respect to the previous

year. No prizes for guessing that the biggest increase was reported in Africa, whose inhabitants are only now starting to discover what the Internet is. Despite this, only 34% of people in Africa has Internet access, whereas in Europe it amounts to 80%. In 2019, there are 3.48 billion social media users, while the total global growth noted year-to-year was 288 million (9%), with 3.26 billion people using social media on mobile devices.

The Internet is a valuable and needed medium used for practically all everyday activities, such as making and keeping in touch with friends on social media, shopping, relaxing, learning or working. A number of people seek physical and mental health advice or ways to express themselves online.

It is said increasingly more often that e virtual reality can no longer be distinguished as a separate sphere of life. Online and offline worlds continuously overlap, and there are scopes in which there is more activity in cyberspace than there is in real life, especially with respect to young people. Sadly, the virtual world of the Internet entails additional security challenges. The increasing transfer of professional and private lives onto the web and prolonged time spent online multiple related risks. The Internet may be a cause of financial and valuable information losses, a source of health issues and emotional disturbances, and it may have a negative impact on our view of the world and the moral sphere (Grabowska, 2017).

This article presents the results of the research conducted among a group of Internet users in three countries: Spain, Poland and Turkey. The objective of this article is to analyze the methods of Internet use from the perspective of user safety.

2. The Review of Literature Concerning Risks of Internet Usage

Internet safety is a complex and non-uniform area, which at the same time constitutes a vital social issue (Mason 2017). This is because threats related to Internet usage cover both the content found online, dangerous contacts, and one's own conduct online. (Livingstone et all, 2011; Włodarczyk, 2013).

Dangerous content may be two-fold. On the one hand, it may be content prohibited by the law. Examples comprise child pornography, racism, and xenophobia. On the other hand, there is legal content (brutal scenes, violence, pornography, promotion auto-destructive behavior, such as drug use, extreme dieting, or even bomb construction or suicide tutorials). Those who publish such content, even though they are harmful, relate to the principles of the international law, i.e. human rights protection, including the right to freedom of expression. This guarantees any individual the right to share an opinion and to disseminate content which others may consider inappropriate.
It shall be highlighted that the Internet is thereby one of the principal methods of terrorist propaganda dissemination (UNODC, 2012).

We should stress that what is considered harmful depends on cultural differences. Every country may reach its own conclusions with respect to drawing a line between what is allowed and what is not permissible (Youth Justice Commission 1996). Oftentimes, one comes across dangerous content accidentally, as an effect of misleading Internet search results or incorrect descriptions of files downloaded in P2P services. The common feature of all negative content is that the contact therewith may have a damaging effect on the human psyche and development, above all (Makaruk, and Wójcik, 2012):

- falsified image of the world,
- distorted physical and mental development,
- emotional disturbances,
- promotion of bad habits,
- loss of the sense of security.

One of the underlying online activities is making and staying in touch with friends. Online contacts may pose a real hazard, in particular when they lead to meetings in the real world. The opportunities the net presents are used, among others, by pedophiles, representatives of various sects, terrorist organizations, Neo-Nazi movements etc. Here, it is worth highlighting that the Internet is the most popular way of establishing relations, recruiting, and winning support by terrorist organizations (Guadagno et al., 2010). In the context of hazardous contacts, the more and more frequently reported dangerous phenomenon online is to induce young people to commit suicides. For instance, within in the first six months of the 2018 alone, the Internet Hotline Centre in Japan received 1329 reports of online sites including disturbing phrases, such as "Let's die together", requesting to remove information in 1255 of them (Jiji, 2019).

Internet activity sometimes leads to cyberbullying. Cyberbullying is referred to as "an act that is carried out by an individual or a group, using electronic communication technologies, repeatedly and over time against a victim who cannot defend him or herself" (Berlińska, and Sztuster, 2014). In practice, cyberbullying is built around stocking, bullying, harassing, and ridiculing other people with the application of tools such as: text messaging, online communicators (WhatsApp), email, websites or closed groups and discussion fora.

This is a particularly dangerous phenomenon, for it features (De Souza Costa Ferreira, Ferreira Deslandes,2018):

- high level of offender anonymity;
- high speed of dissemination of materials aimed at the victim;
- wide availability of such materials;
- constant exposure to attacks, irrespective of one's location or the time of the day/night;
- a relatively low level of social control.

Using the network also poses the risk of cybercrime. Cybercrime covers any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them (UN, 2000). Many authors and institutions, when defining cyber security, cover a wide range of criminal behavior (ITU, 2012; Gercke, 2008). This involves that the definition of cybercrime will continue to evolve along the opening of novel methods allowing cybercriminals attack consumers in new ways. A cybercriminal may use computer devices for unauthorized access or hacking into an email or social network to access a user's personal information, to steel payment information or their identity. They can also commit credit or debit card fraud, make a purchase online that turned out to be a scam, or may infect a device by a virus or other security threat. In the Norton Cyber Security Insights (2017) report, cybercrime is defined as one or more events from a defined list of 20 potential crimes. A cybercrime victim is a person, who confirmed one or more of these events took place.

According to the International report (Digital 2019), the average Internet user spends more than one-quarter of his life online. Additionally, the same report points out that Internet users spend an average of 6 hours 42 minutes online per day, whereas the residents of the Philippines - with the highest Internet use rate - spend online as many as 10 hours 2 minutes every day. The recent rapid development of the Internet has had an immense effect on communication and interpersonal behavior, leading to pathological Internet use (addiction).

Internet addiction is described as an impulse control disorder and is very similar to pathological gambling. To employ pathological gambling as a model, Young (1996) has developed eight criteria positions of Internet addiction. Patients are considered "addicted" if they have provided a "Yes" answer to five or more questions (Sato 2006).

Addiction to the Internet is a broad term encompassing a number of behaviors and issues with managing impulses related to the Internet, personal computer and mobile technologies. Researchers have identified

five subcategories of certain types of computer and Internet addictions (Hoeg, 2019; Akin 2017):

1. Cybersex Addiction.
2. Net Compulsions.
3. Cyber (Online) Relationship Addiction.
4. Compulsive Information Seeking.
5. Computer or Gaming Addiction.

The problem of Internet addiction is especially hazardous when it comes to children and teenagers, for - due to their immaturity - they become addicted much faster than adults do. It is estimated that at present there are between several and over a dozen percent of Internet addicts, and about one-third is at risk of becoming addicted (Paszkowska, 2018).

3. The Objectives and Description of the Research Sample

The study was conducted over the period 2018-2019 on a group of 562 Internet users originating from three countries: Spain, Poland and Turkey.

The purpose of the research was to indicate the methods in which individuals from the respective countries use the Internet and safety implications posed by the more and more popular Internet use.

The first two countries in which the survey was conducted are quite often compared in economic terms (efficiency of using EU funds, development of infrastructure or general economic development) due to the similar size of population or area. Importantly, the percentage of people using the Internet for e-commerce in these countries is also similar and in 2018, it fluctuated in the range of 60% (Eurostat 2019). In turn, Turkey, has developed dynamically over the last several years (Hergül, 2014), and has a level of GDP per capita similar to Poland (Eurostat, 2018). In recent years, Turkey has also been the second fastest growing e-commerce market after India (Deloitte, 2018). On the other hand, Spain is a southern European country, Poland is located in Central-Eastern Europe, and Turkey is at the crossroads of European and Asian cultures. An analysis of the behavior of Internet users from the perspective of cultural differences prove to be look interesting.

The structure of the research sample based on nationality, gender, age, place of residence, and activity is presented in Table 1.

Table 1.
Characteristics of the research sample

Country	
Spain	34.04%
Poland	34.57%
Turkey	31.39%
Gender	
Female	56.17%
Male	43.83%
Activity:	
Lower secondary or primary school student	0.18%
Secondary school student	4.26%
University/College student	37.83%
Professional	57.55%
Pensioner	0.18%
Place of residence.	
100-500,000 inhabitants	17.08%
26-50,000 inhabitants	10.68%
51-100,000 inhabitants	26.33%
over 500,000 inhabitants	25.80%
Village or town of less than 25,000 inhabitants	20.11%
Age of Respondents	
under the age of 18	3.75%
18-24	30.21%
25-34	32.46%
35-44	21.20%
45-54	8.07%
55-64	3.38%
65+	1.13%

Source: own research.

The survey was conducted in electronic form, and information about the survey was provided mainly via social media. Consequently, the age structure of the respondents is similar to the age structure of social media users presented in the report found in the global research (Digital, 2019) (Figure 1).

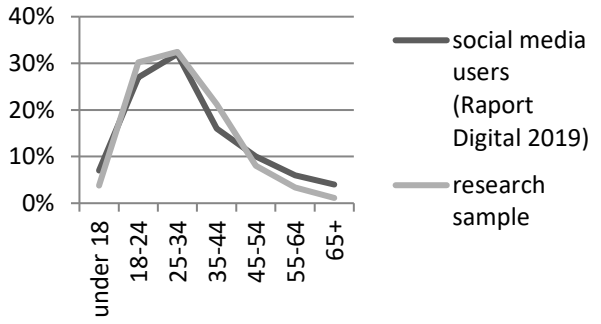

Figure 1. Comparison of the age distribution of the research sample with that of the users of Social Media according to the Digital 2019 Report. Source: own research.

The presence of correlations between the undertaken actions and events breaching information security was verified with the use of the χ2 independence test in accordance with the following formula (1).

$$\chi^2 = \sum_{i=1}^{n} \frac{(0_i - E_i)^2}{E_i} \quad (1)$$

Where:
O - observed value, E - expected value

The expected values were determined employing the formula 2:

$$E_{expected} = \frac{(sum\ of\ row)\ (sum\ of\ column)}{(total\ sum)} \quad (2)$$

In order to examine the impact of the above factors, the Cramer's contingency coefficient V (2) was also computed (formula 3).

$$V = \sqrt{\frac{\chi^2}{n(m-1)}} \quad (3)$$

4. The Analysis of the Ways of Internet Use

On average, over 90% of respondents possess both a computer with Internet access, and a mobile phone. The differences between the respondents in individual countries are small with respect to internet connection (2%) or mobile phone possession (4%). However, there are disproportions with regards to possessing a computer. In Turkey, 85.9% of respondents have a computer, in Spain – 92.2% and in Poland – 98%.

The differences presented above do not translate into difference in the way the Internet is used. Despite the fact that in Turkey the computer is owned by the fewest number of respondents, they use the Internet at home slightly more often (46%) than on their mobiles (44%). In the event of the Spaniards, the proportion is inverse (40.5% uses the Internet on their mobile devices, and 39% at home). Considerable differences are reported in the case of the respondents from Poland, where 54% uses mobile internet on their phones, and only 32% at home (Figure 2). These differences may stem from varying mobile internet costs. The cost of 1 GB mobile data is: in Poland – $1.32, in Turkey – $2.2 and in Spain – $3.79 (https://mobirank.pl).

We should further point out that the respondents in Turkey use the Internet at work twice less frequently that the Poles and Spaniards.

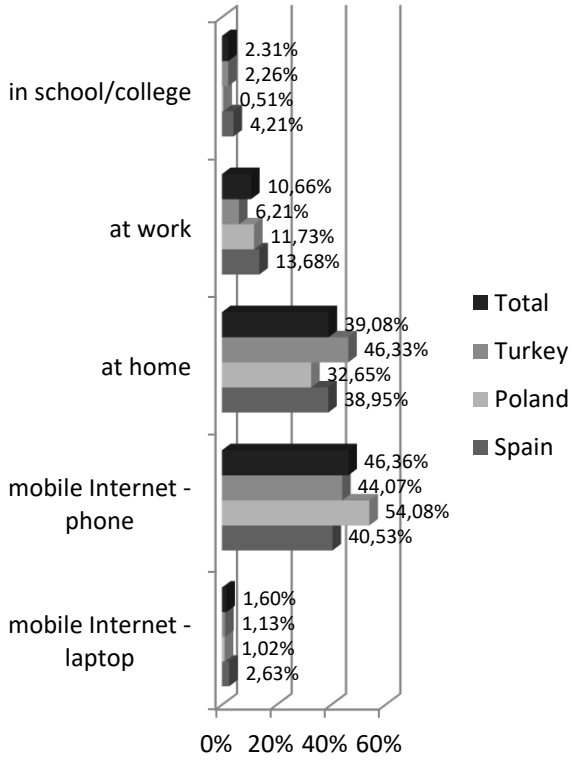

Figure 1. The method of Internet use by respondents' country of origin. Source: own research.

The analysis of the ways of Internet use by gender is also interesting. Nearly 50% of females use the Internet on their mobile phones, and only 37% at home. In the case of males, both of the above methods of Internet use are equally popular (42% each).

The survey demonstrates that it is the Turks who spend most time online. Seventy-five percent of the respondents from Turkey indicated that they spent online over two hours per day. The same answer was provided by 65% of the Poles and 60% of the Spaniards. The differences in online times are also noticeable in the case of division by gender and place of residence. Men and residents of large cities spend more time on the web.

The analysis of answers regarding individual activities conducted online is presented in Figure 3. It is clear that there is a large group of people who use the Internet every day for most applications, of which 44% use it to search for information and to contact their friends (42%) and family (29%). The Internet is also a good way to relax and spend one's free time (33%). What is more, every fourth Internet user does online banking every day. In turn, the least popular activity turned out to be online games, for as many as 28% of the respondents declared that they had never played online.

The analysis of the type of online activity by country of origin reveals that the Poles dominated the majority of aspects. One exception was online games where the Turkish respondents had the lead.

The most popular social media among the respondents was Facebook and Instagram. However, significant differences were recorded with reference to the country of origin. Nearly all respondents from Poland (96%) have a Facebook account. In the interest of comparison, the percentage of Turkish respondents using Facebook was 67%, and Spanish – 60%. Then, as many as 90% of Turks have an Instagram account. The Spaniards were definitely less active (64%) followed by the Poles (only 55%). Even more discrepancies were reported among the Twitter's popularity. Nearly half of the Spanish and Turkish respondents use it (51% and 58%, respectively), in contrast to only 5% of the Polish surveyed. Half of the surveyed population has their own YouTube channel.

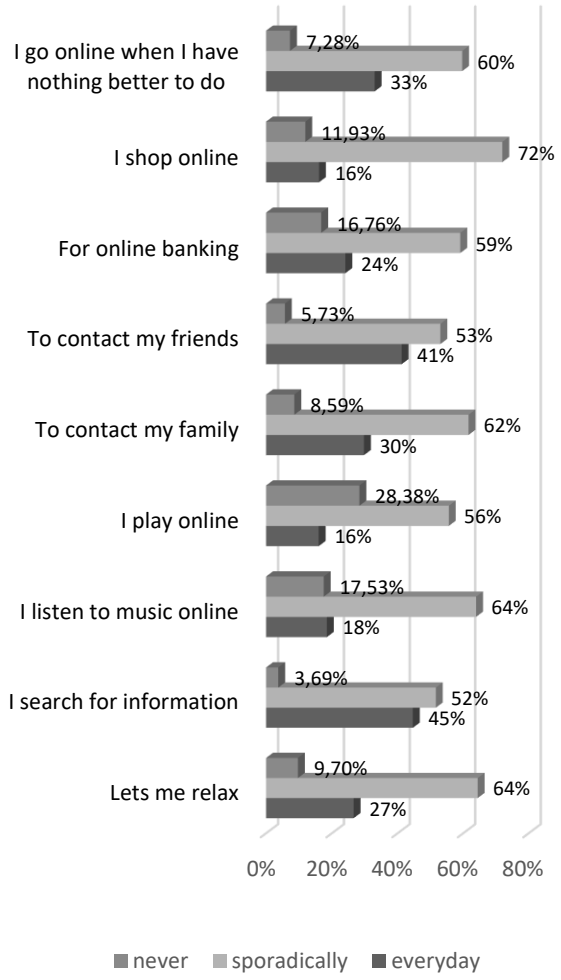

Figure 2. Types of online activity. Source: own research.

More than a half of the respondents with Facebook and Instagram accounts have over 200 friends there and publishes information only about themselves. The most willing to publish information about other people are Spaniards (65%) and the least willing – Turks (38%). Nonetheless, there is no correlation between the readiness to publish information about other people and gender, age or place of residence.

According to the remarks made by the surveyed, Internet use has a significant impact on everyday life changes. As you can see in Figure 4, what is most striking is the reduction of time devoted to watching TV or reading the press, as declared by a half of the respondents. A large group said that they spent less time reading books (33%). Twenty-seven percent of the respondents noticed that being online reduces their time for practicing sports. However, 18% of the respondents observed that information collected from the Internet made them do more sports and read books. The same is the case with family time. Every fourth respondent (26%) noted that online activity reduced family time, and 12% claimed that thanks online activity, the time spent with his/her family extended (e.g. by watching movies or playing games together).

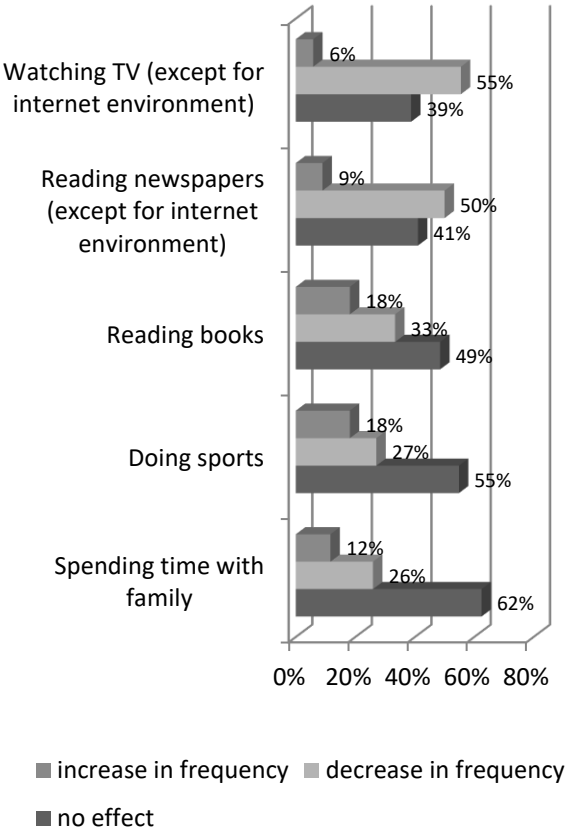

Figure 3. The key changes resulting Internet use. Source: own research.

5. The Analysis of the Consequences of Online Behaviors in the Context of User Safety

Sixty-four percent of the respondents believe that the most considerable risk re-

lating to Internet use is cybercrime (Figure 5).

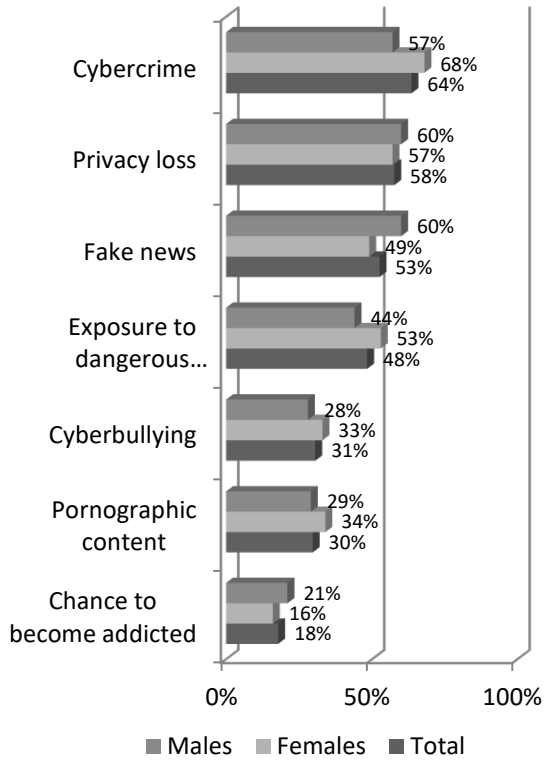

Figure 4. The greatest risk relating to Internet use. Source: own research.

More than a half of the cybernauts fear privacy loss (58%) and untrue information (53%) followed by dangerous content and contact (48%), cyberbullying (31%), pornographic content (30%) and the risk of getting addicted (18%). Nationality (apart from being a victim of a computer crime) had little impact on the distinction between risks associated with using the Internet. Larger differences were observed from the gender perspective.

We can observe a certain paradox here because individuals who perceived a given threat as considerable, experienced it less often. By way of illustration, even though significantly more women (68%) than men (57%) indicated that internet crimes were the most important threat relating to Internet use, men become victims more often (23%) than women (17%). An analogous dependency was seen in the case of privacy loss. It is men who drew more attention to it as a risk (60% vs 58%), whereas real cases of privacy loss (social account takeover) happened more frequently to women (61%) than men (52%).

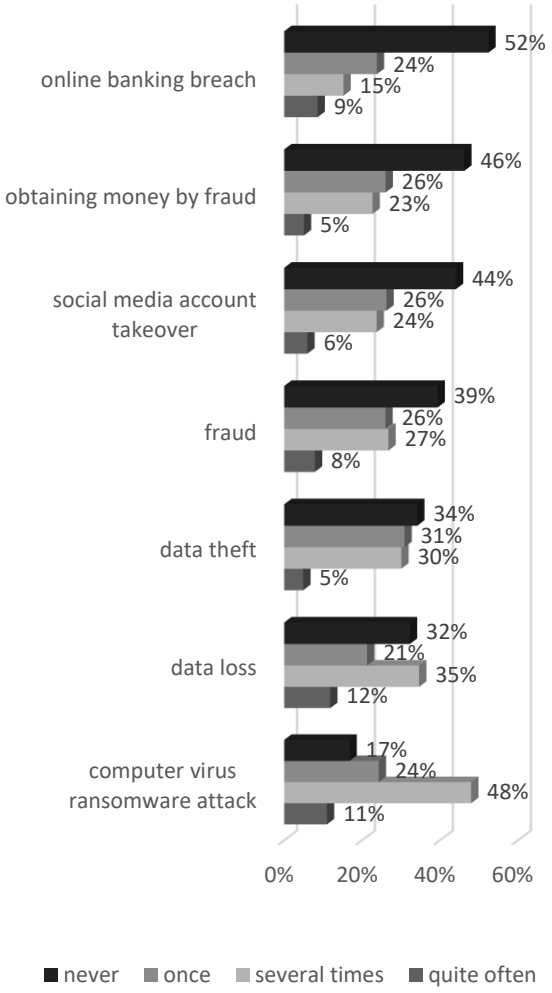

Figure 5. The most frequent security breaches the respondent were the victims of. Source: own research.

Generally, every fifth respondent declared that s/he had been a victim of a cybercrime. The respondents from Spain (23%) were slightly more often affected than those in Poland and Turkey (17% and 18%). The most frequent type of an online activity-related security breach were ransomware attacks and computer viruses. Amongst other common crimes are theft and fraud (Figure 6).

Despite the fact that the chance of becoming addicted was the most rarely indi-

cated the risk of Internet use, only 42% of the respondents had no negative emotions related to not having Internet access. There are notable differences in corresponding answers provided with respect to gender. Insofar as every other women does not experience negative consequences due to the lack of Internet access, as many as 2/3 of men do. The most frequent negative reaction to lacking Internet access is anger and irritation and inability of managing one's time (both answers were selected by 28% of the respondents). The angry reaction is similar in numerical terms for women (27%) and men (27%).However, twice as many men as women (39% to 20%) do not know what to do when they are disconnected from the web (Figure 7).

The analysis of the results from the perspective of the respondents' country of origin demonstrates that the most susceptible to the lack of Internet are the Spaniards (78% of those surveyed from Spain report experiencing negative emotions), while the most resistant to it are the Poles (only every third Pole sees negative emotions as a consequence of no Internet connection).

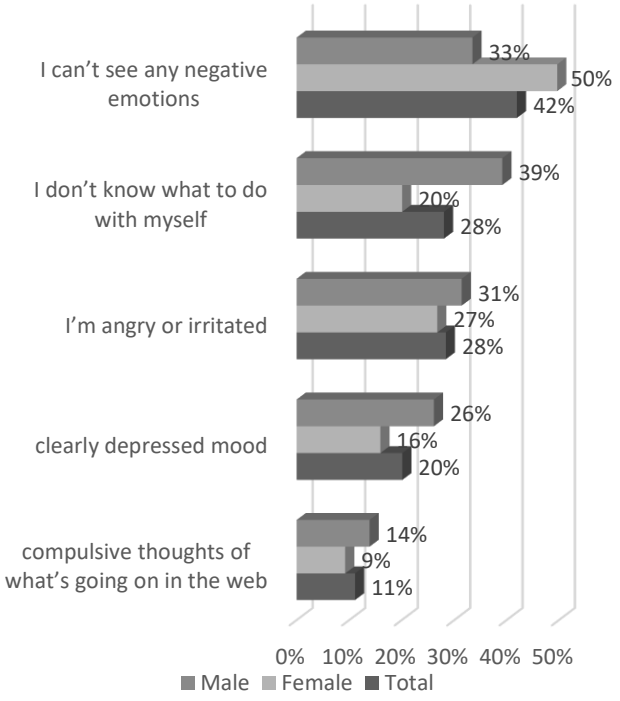

Figure 6. The most frequent negative emotions associated with the lack of Internet access in relation to gender. Source: own research.

6. Information security activities

The majority of the respondents (78%) have installed an anti-virus system on their desktop computers. The situation of mobile phone users is definitely worse. Only 36% of the surveyed who declared to be using mobile Internet most often had an anti-virus installed on their mobiles, whereas there are significant differences between the countries of origin (Figure 8). Nonetheless, no correlation was reported between the fact of installing an anti-virus program and gender, age, or place of residence.

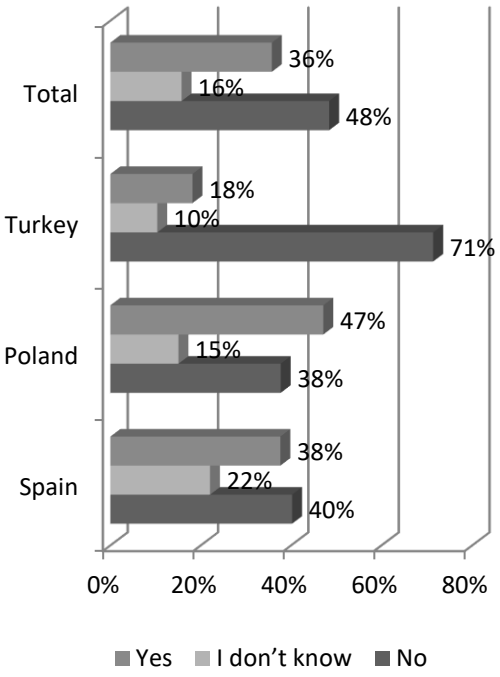

Figure 7. Anti-virus software installed on mobile phones among those who declared to be using mobile Internet most often. Source: own research.

The analysis of the dependencies between having an AV software on one's mobile phone and the fact of being a victim of a cybercrime led to some interesting conclusions. It appears that every third person having an anti-malware on a mobile phone experienced cybercrime. In the event of individuals not having an AV software, the percentage of cybercrime victims was nearly

three times lower and amounted to only 13% .

The relation between having AV software on one's mobile and the fact of being a victim of a cybercrime and its special example – computer virus infection or ransomware attacks – were verified with the use of the χ2 independence test according to the formula (1). In order to examine the impact of the above factors, the Cramer's contingency coefficient V (2) was also computed. The results are presented in Table 2.

Table 1.
The relation between having AV software on one's mobile and the fact of being a victim of a cybercrime

The relation between having an AV software on a mobile phone and:	χ^2 computed	χ^2 for α= 0.05	χ^2 for α= 0.005	V_{cr}
1. Fact of being a victim of a cybercrime	19.5	5.99	10.5965	0.19
2. Fact of being a victim of a ransomware/ virus	57.3	5.99	10.5965	0.57

Source: own research.

As you can see, both for the level of significance α=0. 05 and α=0,005, there is a correlation between having AV software on one's mobile and the fact of being a victim of a cybercrime and its specific case – computer virus infection or ransomware attacks. The computed Cramer's contingency coefficient V (0.57) shows that there is a strong correlation between the fact of being victim of a ransomware attack or a computer virus infection and an anti-virus software installed on one's mobile. In the general example of experiencing cybercrime, this correlation is weak (0.19).

The above result may be interpreted as follows: only first-hand cybercrime experience brings many Internet users to take up protective actions.

The issue of changing social media account passwords is presented equally pessimistically.

As seen in Figure 9, only every third respondent changes his/her password more often than once per six months. In turn, nearly half of the surveyed (48%) do not change passwords to the social media account at all. No differences were observed with respect to the frequency of changing passwords with respect to one's nationality, gender, age, or place of residence.

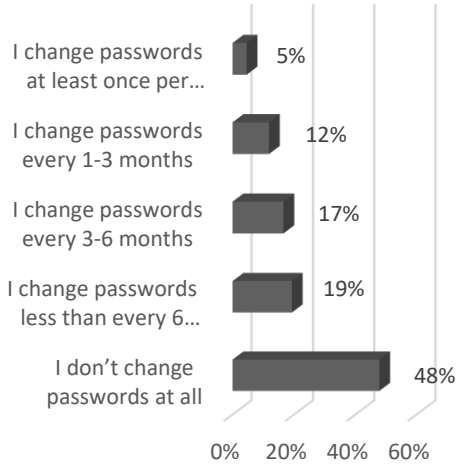

Figure 8. Frequency of changing one's social media account password. Source: own research

The analysis of the frequency of changing one's social media password revealed an identical correlation as in the case an anti-virus software installed on one's mobile. Here, individuals also changed their password definitely more often if they had been victims of cybercrimes. Individuals who have never experienced this are much less eager to change their passwords.

The above correlation was verified with the use of the χ2 independence test. In order to examine the impact of the above factors, Cramer's contingency coefficient V was also computed. The results are presented in Table 3.

Table 2.
The relation between the frequency of changing one's social media password and being a victim of a cybercrime.

The relation between the frequency of social media password change and being a victim of a cybercrime.	χ^2 computed	χ^2 for α= 0.05	χ^2 for α= 0.005	V_{cr}
	52.98	9.48	14.8	0.32

Source: own research.

As you can see, both for the level of significance α=0. 05 and α=0,005, there is a correlation between the frequency of social media account change and the fact of having been exposed to a cybercrime. The determined Cramer's contingency coefficient V (0.32) indicated that there correlation is medium-strong.

With social media in mind, it is reported that solely 25% of the respondents had read and understood the rules and regulations of the social media where they had an account. The above result is similar for both men and women. Forty-two percent had read some of it (women dominate here), and every third individual had failed to do it (men more often than women). The differences in this approach to rules and regulations are also sharp when it comes to the country of origin. Most Poles read the rules and regulations, however to some extent only. Spanish respondents dominate among those who do not read the rules and regulations, whereas Turkish respondents constitute the greatest percentage of those who read the rules and regulations carefully (Figure 12).
What is positive is that only 11% of the respondents publishing content in social media grant unrestricted access to everybody. The remainder either hides some content (58%) or publishes all information as available to friends only (31%).

Only slightly over 40% of the respondents believe that they are well informed about the risks relating to Internet use. Women (43%) prevail over men (38%). Sadly, the analysis of other answers provided by those who believe to be well informed about the risks related to Internet use suggests otherwise. By way of illustration, 50% of those who say that are well informed, have no anti-virus software on their smartphones. In turn, nearly half of the surveeys (46%) does not change passwords to social media account at all.

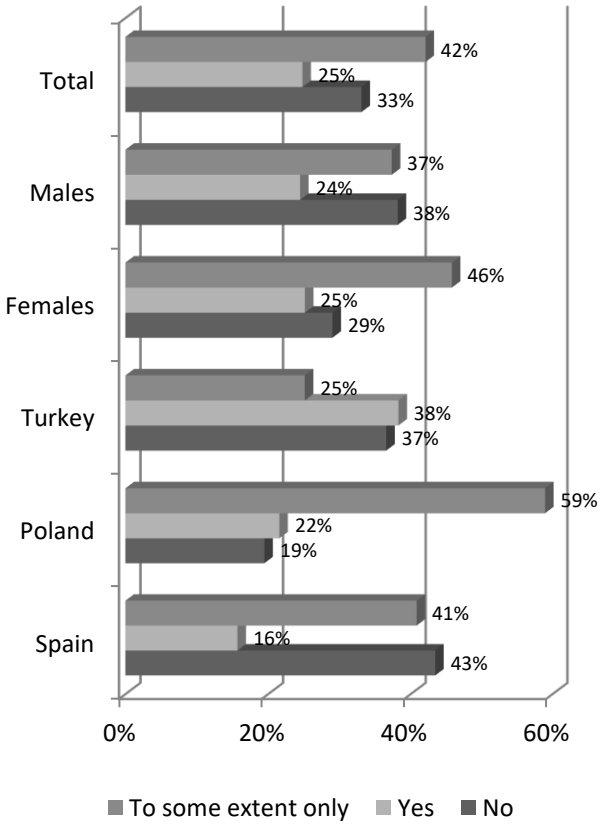

Figure 9. Reading the rules of regulations of social media websites by gender and country of origin. Source: own research.

7. Conclusions

The Internet has become an indispensable part of our lives. Network services use helps us with an increasing number of matters in various fields, absorbing us more and more. Hours spent online makes one devote less time to previous hobbies: TV, newspapers, books, or sports. In addition, new threats appear, jeopardizing individuals' safety.

The analysis of data from respondents from three countries (Spain, Poland and Turkey) indicated that, depending on where they live, they use of the internet in a slightly different way, both from the perspective of the place (home or mobile internet) and preferred social networks. Nevertheless, they face the same threats: crime, computer, loss of privacy, fake news. An interesting observation was the fact that the Spaniards dominated among people who do not read the regulations of the social networks they use and are more than twice as sensitive to the lack of Internet access (78% of respondents from this country notice negative emotions) than Poles (every third Pole perceives the negative emotions associated the lack of Internet).

The respondents from Turkey were in the middle of these rankings, and in turn definitely stood out negatively from the others in terms of anti-virus protection of mobile devices. Perhaps the abovementioned differences can be explained by different cultural conditions and, consequently, a different level of emotional expression, or normative regulation (Lim, 2016). However, this requires further empirical verification.

Unfortunately, despite our awareness of the risks related to Internet use and their proper identification, we do little to protect us from them. The data analysis revealed that only first-hand cybercrime experience brings one to take safeguard measures.

Another pessimistic fact is lack of awareness with respect to Internet security. It appears that even those who consider themselves informed in the subject matter fail to demonstrate it in practice.

The growing influence of the Internet on our lives, given the behaviors of the analyzed Internet users, indicates the need to channel our efforts into increasing awareness of safe online behavior.

References

1. Akin, M. (2017). A Research on the Impacts of the Young People's Internet Addiction Levels and their Social Media Preferences. *International Review of Management and Marketing,* 7(2), pp. 256-262. Retrieved from https://www.econjournals.com/index.php/irmm/article/view/4380/pdf, (12 March 2019).
2. Berlińska, J., and Sztuster, A. (2014). *Cyberprzemoc. O zagrożeniach i szansach na ograniczenie zjawiska wśród adolescentów*. Warszawa: Wydawnictwo Uniwersytetu Warszawskiego.
3. Council of Europe (2001). *Organisedcrime situation report 2000*. Retrieved from https://www.coe.int/t/dg1/legalcooperation/economiccrime/organisedcrime/Report2000E.pdf, 10.11.2018.
4. De Souza Costa Ferreira, T.R., and Ferreira Deslandes, S. (2018). Cyberbullying: concepts, dynamics, characters and health implications*, Ciência & Saúde Coletiva*, 23(10), pp.3369-3379. DOI:10.1590/1413-812320182310.13482018.
5. Deloitte (2018). *Report: E-Commerce in Turkey 2017 Market Size*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/TUBISAD_2018%20E-Commerce%20in%20Turkey_EN_final.pdf, 26.04.2019.
6. *Digital 2019. Global Digital Overview* (2019). Retrieved from https://www.digitalinformationworld.com/2019/02/internet-users-spend-more-than-a-quarter-of-their-lives-online.html, 04.04.2019.
7. Eurostat (2018). *Consumption per capita in purchasing power standards in 2017.* Retrieved from

https://ec.europa.eu/eurostat/documents/2995521/9447627/2-13122018-AP-EN.pdf/5975f52d-b92b-448d-8c5c-0532a4d50430, 08.02.2020.
8. Eurostat (2019). *E-commerce statistics for individuals*. Retrieved from https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46776.pdf, 12.03.2020.
9. Gercke, M. (2008). National, Regional and International Approaches in the Fight Against Cybercrime *Computer Law Review International,* 9(1), pp. 7-13.
10. Gordon, S., and Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*, 2(1), pp. 13-20. DOI: 10.1007/s11416-006-0015-z.
11. Grabowska, M. (2017). Zagrożenia dzieci i młodzieży w Internecie. *Studia i prace pedagogiczne,* 4, pp. 137-144.
12. Guadagno, R.E. et al. (2010). Social Influence in the online Recruitment of terrorists and terrorist Sympathizers: Implications for Social Psychology Research. *Revue internationale de psychologie sociale*, 23(1), pp. 25-56.
13. Hergül, S. (2014). *Turkish Online Startups & E-commerce in Turkey*. Retrieved from https://www.slideshare.net/sezginhergul/turkish-online-startups-ecommerce-in-turkey, 14.09.2018.
14. Hoeg, N. (2019). *What Is an Internet Addiction?* Retrieved from https://www.addictioncenter.com/drugs/internet-addiction/, 27.04.2019.
15. ITU (International Telecommunication Union Telecommunication Development) (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Geneva: Switzerland Telecommunication Development Sector.
16. Lim, N. (2016). Cultural differences in emotion: differences in emotional arousal level between the East and the West. *Integrative Medicine Research*, 5(2), pp.105-109. DOI:10.1016/j.imr.2016.03.004.
17. Livingstone, S. et al. (2011). *Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries.* EU Kids Online, Deliverable D4. EU Kids Online Network, London, UK. Retrieved from http://eprints.lse.ac.uk/33731/1/Risks%20and%20safety%20on%20the%20internet%28lsero%29.pdf, 19.09.2019.
18. Makaruk, K., and Wójcik, Sz. (Eds.) (2012). *Badanie nadużywania internetu przez młodzież w Polsce i Europie*. Retrieved from http://www.saferinternet.pl/pobierz.php?i=3&hash=460f, 05.02.2019.
19. Mason, M. (2017). *The use of the internet and social media by young people*. Retrieved from https://www.researchgate.net/publication/315658325_The_use_of_the_internet_and_social_media_by_young_people, 20.10.2019.
20. *Norton Cyber Security Insights Report* (2017). Retrieved from https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf, 01.11.2018.
21. Paszkowska, E. (2018). *Bezpieczny Internet*. Retrieved from https://www.google.pl/zagrożenia+w+internecie+prezentacja, 10.10.2018.
22. Sato, T. (2006). Internet Addiction among Students: Prevalence and psychological problems in Japan. *Japan Medical Association Journal 'JMAJ'*, 49(7/8), pp. 279–283.
23. Jiji (2019). Japanese police step up cyberpatrols to counter growing amount of online info urging suicide. *The Japan Times*. Retrieved from https://www.japantimes.co.jp/news/2019/05/29/national/social-issues/japanese-police-step-cyberpatrols-counter-growing-amount-online-info-urging-suicide/#.Xe4KjuhKi1s, 30.09.2019.
24. UN (Congress on the Prevention of Crime and the Treatment of Offenders Crimes related to computer networks)

(2000). *Background paper for the workshop on crimes related to the computer network*, A/CONF.187/10. Retrieved from www.uncjin.org/Documents/congr10/10e.pdf, 23.11.2018.
25. UNODC (United Nations Office on Drugs and Crime) (2012). *The use of the Internet for terrorist purposes*. New York: United Nations. Retrieved from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, 15.12.2018.
26. Williams, F.P. (2005). Cybercrime. In Miller, J.M., and Wright, R.A. (Eds). *Encyclopedia of Criminology*. New York: Routledge.
27. Włodarczyk, J. (2013). Zagrożenia związanie z korzystaniem z internetu przez młodzież. Wyniki badania, EU NET ADB. *Dziecko Krzywdzone. Teoria, badania, praktyka,* 12(1). pp. 49-68.
28. Wójcik, S. (2017). Zagrożenia dzieci i młodzieży w internecie. *Dziecko Krzywdzone. Teoria, badania, praktyka*, 16(1), pp. 270-287
29. Young, K.S. (1996). *Caught in the Net: How to Recognize the Sign of Internet Addiction and a Winning Strategy for Recovery*. New York: John Wiley & Sons.
30. Youth Justice Commission (of the European Communities) (1996). *Illegal and harmful content on the Internet*. Retrieved from http://aei.pitt.edu/5895/1/5895.pdf, 15.08.2019.