

# Risks Inherent in Inaccurate or Inadvertent Use of Social Networks in Greece

Eleni Stratigopoulou, Klimis Ntalianis, Vasiliki Kikili, Filotheos Ntalianis

**Abstract**— Social Networking Websites are not only the most widely used tools to facilitate communication in today's digital age, but they are also one of the biggest sources of Big Data. There are of course many benefits of data applications, for both ordinary users and professionals alike, but also there are many risks, that users of Social Networking Sites can face. As users' interest in using Social Networking Websites grows, so does their concern about the risks they pose. The purpose of this thesis is to investigate the risks posed by the use of Social Networking Websites to adult users in Greece and examine the behaviors of users that may lead to risk exposure, (behaviors such as Risk Taking, Privacy Behavior, Trust in SNS companies, Privacy Concern, Perceived Control of Information, Information Identity Disclosure will be examined). It will also examine the correlation of user behaviors and exposure to risk and socio-demographic data of users. The results of the present study show that exposure to Risk in SNS is related to gender and also "Privacy Behavior" and "Information Identity Disclosure" are related to Age and Educational Level.

**Keywords**— Social Network, Online Dangers / Risks / Threats, Privacy, Cyber-bullying, Careless Use of Internet.

## I. INTRODUCTION

THE internet and social networks are part of the daily lives of a large part of the national as well as the global population, as their communication capabilities are enormous. Worldwide users within a decade have grown from almost one billion in 2010 to 2.8 billion in 2019 [1] (Clement, 2019). Correspondingly, in recent decades the flow of information has also increased. As reported by Hilbert et al. (2016) [2], information exchange capability has increased from the equivalent information of two newspaper pages per person per day in 1986 to six whole newspapers in 2007, with Google able to handle approximately 2,000,000 search queries in just one minute, while users of Facebook can share about 700,000 pieces of content, respectively. All this information however apart from the benefits it can offer (education, information, exchange of experiences between individuals, business-to-

This work was supported in part by Interbit Research (<http://www.interbit-research.com/>).

E. Stratigopoulou is with the Open University of Cyprus, 3, Giannou Kranidioti Ave., 2220, Latsia, Nicosia, CYPRUS (e-mail: [eleni.stratigopoulou@st.ouc.ac.cy](mailto:eleni.stratigopoulou@st.ouc.ac.cy), [estratigopoulou@gmail.com](mailto:estratigopoulou@gmail.com)).

K. Ntalianis is with the Department of Business Administration, University of West Attica, Egaleo, Athens, Greece (e-mail: [kntal@uniwa.gr](mailto:kntal@uniwa.gr)).

V. Kikili is with the Ministry of Education and Religious Affairs, Directorate of Primary Education, Athens, Greece (e-mail: [vasikik@gmail.com](mailto:vasikik@gmail.com)).

F. Ntalianis is with the Department of Business Administration, University of Piraeus, Piraeus, Greece (e-mail: [filotheos@unipi.gr](mailto:filotheos@unipi.gr))

business relationships, environment and medium for new approaches and channels of communication and more), however, it is a source for criminals, and generally abusive behavior. That is, it poses risks to the Personal and Digital Security of the individual. The "Cambridge Analytica Scandal", when it gained access to Facebook users' data in 2014, is partly proof of the risks involved, and more specifically in this case, of violating the privacy of Social Networking Websites users, (through the terms of use privacy of Facebook or other SNS's- the privacy of users is not necessarily guaranteed, as much of the disclosed information is also disclosed by the users themselves in their interaction) (Todd, 2018, [3]), (González-Bailón, 2018, [4]). But there are other cases like the aforementioned, including the example of a breach of the privacy of Sony users in 2011 (Social Media and Our Privacy, 2016, [5]). The issue of the security of social networking users, the breach of their personal data and other risks arising from the breach of personal data of users is a concern that necessarily accompanies the use of social networking sites by both users and researchers ("Today's social network sites," 2017, [6]).

The dangers that have occasionally been reported to arise from the use of technology and social networks are many and are constantly renewed. The effects, which can have on the individual, vary not only from the encounter of strangers, which was and is a great fear of the interaction of people who do not know each other, but also of the risks involved in disclosing personal information. It should also be noted that much of the technology-related risks associated with Social Networks involve risks related to Private Life and Privacy.

Risks affecting social network users are categorized into 4 different categories. The first category relates to privacy and security risks (classic threats). The second category concerns new risks affecting Social Networking infrastructure and Social Networking infrastructure itself is being used to undermine the privacy and security of Social Media Users. The third category is a combination of threats to bring greater risks. The fourth category mainly deals with risks related to children and through the social media (Fire et al., 2014, [7]).

Classic threats concern the use of the user's personal information provided on the Social Network (s) that interacts, with final aim of attacking the user and his/her friends, using the user's personal information accordingly. Such threats include malware, spam, phishing attacks, Spammers, Cross-Site Scripting (XSS), internet scams. These risks, although not new, are still a major problem, as they are rapidly expanding

due to the structure and nature of Social Networks. The purpose of the risk is the user's personal information, such as information related to bank accounts, credit card numbers, security codes, and in some cases the target becomes the bandwidth itself of user's network, in order to use it - to send spam emails (Fire et al., 2014, [7]).

**Modern Threats /Risks-**They are threats related to the social networking environment and are aimed at the personal information of the user and his/her contacts. The intruder in any case tries to connect with the user and his/her contacts, creating a fake profile and initiating a friendship request with a targeted user. Upon acceptance by the user of the intruder, his data, are also exposed to the attacker. Privacy and ultimately the security of the user is the goal of this risk category. Such threats include Click-jacking, De-Anonymization Attacks, Fake Profiles, Identity Clone Attacks, Inference Attacks, Face Recognition, Information Leakage, Location Leakage, Socware (Fire et al., 2014, [7]).

**Combined Threats -**Combining threats against the user, is a way an attacker can use to create a more sophisticated attack. This implies old and new forms of threats. For example, the use of Internet fishing to extract a password or security codes and then by posting a message on the user's log (click-jacking), prompting the user to click on the post, to install a hidden virus on their computer(Fire et al., 2014, [7]).

**Risks and Threats to Children -** Many of the Social Network Sites are intended for use by adolescents and adults, some of them have no age limit and some are aimed at children. It is undeniable that Social Network Sites offers many opportunities to young people but at the same time they are also associated with risks.

Users of Social Networks of all ages are exposed to all the above-mentioned threats and risks. However, children and adolescents are also a completely different target and are exposed to other risks. Online Predators, Risky Behaviors, Cyber-bullying (& Cyber abuse), (Fire et al., 2014, [7]).

The purpose of this study is to investigate the classic risks posed by the use of Social Networking Websites to adult users. The expected results of the research include the determination of the degree of the penetration of the use of Social Networking Websites to Internet users, to examine the behaviors of users that may lead to risk exposure (behaviors such as Risk Perception will be examined, Privacy, Trust in SNS companies, Privacy Concerns, Perceived Control of Information, Identity Information Disclosure).

To fulfill the scope of the study, the following research questions were stated:

1. Which are the most popular (dominant) Social Networking Platforms.
2. What is the degree of penetration (use) of Social Networks to Internet users.
3. What are the most common risks in Social Networks Sites and exposure factors?
4. Is there a relationship between Socio-demographic characteristics of SNS's users and risk-taking behaviors?
5. Is there a correlation between the socio-demographic characteristics of users of social networking sites (gender, age,

educational level) and exposure to online risks?

## II. RELATED WORK

The study of the literature reviewed regarding the risks on social networking sites showed that the vast literature-international and Greek-, mainly focuses on risks, such as addiction in children and young adults, but also risks such as cyber-bullying and sexual harassment. When the literature focuses on risks in Personal life it examines mainly Problematic Internet Use and feelings such as depression, neurotism etc, that users feel as a result of Internet use. Various research studies have examined different aspects and dimensions of the topic of risks either in Internet or in SNS and these are: International Literature addiction Internet or Social Networking Sites: (Young, Kimberly S., 1996, [8]), (Lee et al., 2015, [9]), (Bányai et al., 2017, [10]).

International Literature SNS Risks in Personal life, Cyber-bullying, and other risks in Internet and SNS: (Ponte et al., 2013, [11]), (Ybarra et al., 2006, [12]), (DeMarco et al., 2017, [13]), (Debatin et al., 2009, [14]), (Fogel & Nehmad, 2009, [15]), (Christofides et al., 2012a, [16]), (Christofides et al., 2012b, [17]), (Saeri et al., 2014, [18]), (Kezer et al., 2016, [19]), (Meter & Bauman, 2015, [20]), (Sampasa-Kanyinga & Hamilton, 2015, [21]), (Mitchell & Ybarra, 2009, [22]), (Livingstone & Brake, 2010, [23]), (Weir et al., 2011, [24]), (Hongyu Gao et al., 2011, [25]), (Vandoninck et al., 2012, [26]), (Ephraim, 2013, [27]), (Hajli & Lin, 2016, [28]), (Montes-Vozmediano et al., 2018, [29]).

Greece Literature Internet Generally Addiction & Problematic Internet Use: (Tsitsika et al., 2009, [30]), (Frangos et al., 2011, [31]), (Kormas et al., 2011, [32])

Greece Literature Internet Bullying and Risks in General: (Floros et al., 2013, [33]), (Antoniadou & Kokkinos, 2015, [34]), (Gkiomisi et al., 2017, [35])

Greece Literature SNS Risks in Personal Life, Bullying and Risks in General: (Giota & Kleftaras, 2013, [36]), (Kourouthanassis et al., 2015, [37]), (Tsiolka et al., 2017, [38]).

The study of existing international literature mainly focuses on risk issues such as bullying but also on specific age groups such as those of children and adolescents (Ybarra et al., 2006, [12]), (DeMarco et al., 2017, [13]), (Kezer et al., 2016, [19]). The National Greek Bibliography, respectively, focuses mainly on risk issues related to Problematic Internet use (Tsitsika et al., 2009, [30]), (Kormas et al., 2011, [32]), also searches reasons for using Social Networking Web sites, and bullying, also in young people and children mainly (Gkiomisi et al., 2017, [35]), (Antoniadou & Kokkinos, 2015, [34]). Research of other risks in SNSs in Greece is very limited. According to published statistics, social network users in 2019 was 45% of the global population with approximately 2.65 billion users. The corresponding figure in 2010 was about 1 billion users. Increased use of devices such as telephones, also facilitates access to SNS (Clement, 2019, [1]). The expansion as well as the proliferation of Social Networking Websites and their penetration into a growing part of the adult population, (not only nationally but also globally), almost makes it

necessary to carry out the proposed research, - global SNS's users in 2021 is expected to be about 3.1 billion (Clement, 2019, [1]), (infographic – information – technologies – 2019 — ELSTAT, n.d., [39]) (Greece in Numbers—ELSTAT, n.d., [40]). Greece's population age distribution, according to the 2011 census, as well as from other estimates published in the press, reinforces the view that the Greek population tends to be at an adult rate higher than in older times (Statistics - ELSTAT, n.d., [41]) ("Statistics," n.d., [42]), (Salourou, 2015, [43]).

The purpose of this research proposal is to fill the existing gap in the existing literature on risk detection on Social Networking Sites in the adult population in Greece.

### III. RESEARCH PREREQUISITES

This study uses the quantitative method to collect data, as through these data and the results that were obtained, exposure to risk factors can be examined, and if and how much the user of SNS's perceives exposure to risk. Research is targeted in adults of age of 18+, as those ages are less likely to be examined than children and adolescents.

Non-Random Sample of Approximately 4,000 People. Participating adults over 18 years of age. Greece is the place where the research was conducted.

The questionnaires were created through the Google forms and distributed in two different ways, 1. via the Facebook Social Networking application and 2. via Gmail. 1. Facebook friends was invited to fill out the questionnaire, but also asked them to post the questionnaire on their wall, asking their own "friends" to fill it out - snowball method. 2. E-mail messages were sent to employees in a large public organization. Both the text of the Facebook post and the accompanying e-mail to the prospective participants contained information on how to maintain the participants' anonymity (both on completing the questionnaire and on collecting data). In order to send the questionnaires to the e-mail addresses to recipients of Large Public Organization, permission was requested and obtained electronically by the Management of the organization. Pilot implementation period 17/07/2019 - 20/07/2019. Period of implementation of the survey 21/07/2019 - 23/09/2019.

The questionnaire was eventually filled out by 432 persons, of which 98 did not hold an SNS account.

The subscales used are:

Use of Social Networking Websites - 9 item General Social Media Usage Subscale, of the "Media Technology Usage and behavior Scale - MTUAS", on 10th Likert scale from 10 from 1 = Never to 10 Continuous/ All Time (Rosen et al., 2013, [44]). Reliability of Initial Questionnaire Cronbach Alpha 0.60-0.85. Reliability of Pilot Questionnaire Cronbach Alpha 0.861. Reliability of Research Questionnaire Cronbach Alpha 0.852.

Personal Information Sharing Practices (PISP) in SNS Questionnaire (Ball et al., 2015, [45]), with Yes / No answers

Risk Averseness Scale was measured using the 5 item questionnaire of Pan & Zinkhan (2006) [46], (Fogel & Nehmad, 2009, [47]). Questions are rated on a 5 / Likert scale from 1 = Strongly Disagree to 5 Strongly Agree. Reliability of

Initial Questionnaire Cronbach Alpha 0.76. Reliability of Pilot Questionnaire Cronbach Alpha 0.875. Reliability of Research Questionnaire Cronbach Alpha 0.795.

Trust in SNS Companies was measured using the 4 item questionnaire of Pan & Zinkhan (2006), [46], (Fogel & Nehmad, 2009, [47]). Questions are rated on a 5 / Likert scale from 1 = Strongly Disagree to 5 Strongly Agree. Reliability of Initial Questionnaire Cronbach Alpha 0.95. Reliability of Pilot Questionnaire Cronbach Alpha 0.949. Reliability of Research Questionnaire Cronbach Alpha 0.895.

Privacy Behavior Scale was measured with 6 item questionnaire of Buchanan, et al (2007), [48], (Fogel & Nehmad, 2009, [47]). Questions are rated on a 5 / Likert scale from 1 = Never to 5 Always. Reliability of Initial Questionnaire Cronbach Alpha 0.80. Reliability of Pilot Questionnaire Cronbach Alpha 0.944. Reliability of Research Questionnaire Cronbach Alpha 0.790.

Privacy Concern Scale was measured using the 3 item questionnaire of Dinev & Hart, (2004), [49], (Fogel & Nehmad, 2009, [47]). Questions are rated on a 5 / Likert scale from 1 = Strongly Disagree to 5 Strongly Agree. Reliability of Initial Questionnaire Cronbach Alpha 0.92. Reliability of Pilot Questionnaire Cronbach Alpha 0.763. Reliability of Research Questionnaire Cronbach Alpha 0.916.

Perceived Control of Information was measured using the 3 item questionnaire of Krasnova et al. (2010), [50], (Hajli & Lin, 2016, [28]). Questions are rated on a 5 / Likert scale from 1 = Strongly Disagree to 5 Strongly Agree. Reliability of Initial Questionnaire Cronbach Alpha 0.89. Reliability of Pilot Questionnaire Cronbach Alpha 0.932. Reliability of Research Questionnaire Cronbach Alpha 0.830.

Identity Information Disclosure Scale was measured with questionnaire of Stutzman, (2006), [51], (Fogel & Nehmad, 2009, [47]), which contains 2 sub scales 4 item, each. Questions are rated on a 5 / Likert scale from 1 = Strongly Disagree to 5 Strongly Agree. Sub scale A: Reliability of Initial Questionnaire Cronbach Alpha 0.82. Reliability of Pilot Questionnaire Cronbach Alpha 0.813. Reliability of Research Questionnaire Cronbach Alpha 0.736. Sub scale B: As Scale Reliability is not the same in both questionnaires - Cronbach Alpha 0.813 in A questionnaire while B's questionnaire Cronbach Alpha was low, the items of B questionnaire were analyzed autonomously.

All questionnaires were translated and adapted to Greek by the researchers.

IBM SPSS v26 for iMac was used for data processing, statistical analysis, output of tables, images and graphics.

### IV. EXPERIMENTAL RESULTS

Of the 432 participants, 294 (68.1%) were women and 138 (31.9%) were men. The age composition of the sample is: the age group of 18-28 consisted of 42 (9.7%) persons, the age group of 29-38 years, 82 (19%) persons, the age group of 39-48 years consisted of 150 (34.7%) persons, the age group of 49-68 consisted of 157 (36.3%) persons and 1 (0.2%) person in the category of 69+ years. In terms of education level, 3 (0.7%) persons had Compulsory Education (up to 3rd Grade),

59 (13.7%) had Secondary Education (High School), while 370 (85.6%) had Higher Education.

Regarding research question for degree of penetration (use) of Social Networks to Internet users results, Figure 1 shows that 334 (77.3%) persons participate in Social Networking Sites, while 98 (22.7%) do not participate. As the 98 persons, out of 432 participants, do not have an account in Social Network Sites, those 98 persons, after the specific question, for the remaining (and related social networking questions), were excluded from the analysis of results. So, the analysis only applies to the 334 persons who eventually have an account on Social Networking Sites.

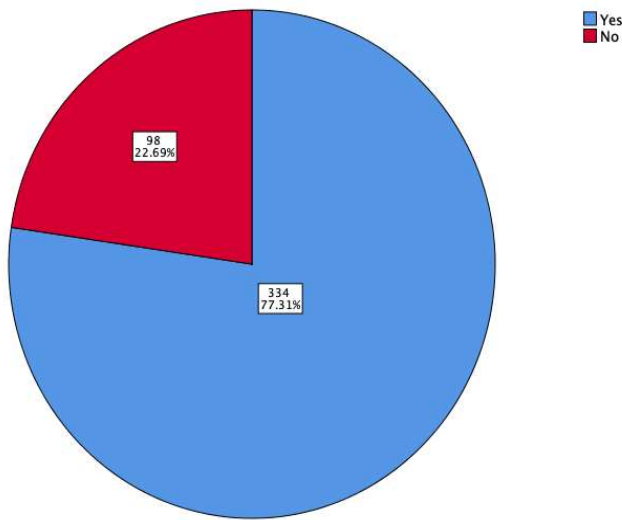


Fig. 1 Participation in Social Network Sites

Regarding results on the most popular (dominant) Social Networking Platforms, it appears in Figure 2, 95.2% of users have a Facebook account, (which show that is the most popular Website) with the next one being YouTube, which gathers preference of the 54.8% of users.

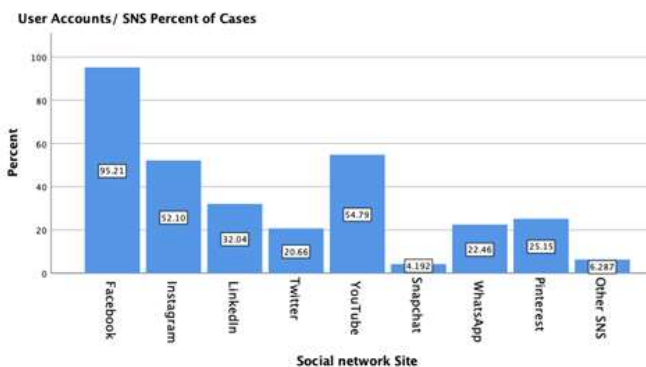


Fig. 2 Most Popular SNSs

Moreover, participants maintain one (1) up to nine(9) different accounts in SNS's, as it appears in the Figure 3, with most common case to be with accounts in two (2) different SNS 27,2% and the next one with three (3) different SNS

accounts 22,5%.

Regarding research question 3 about the most common risks in Social Network Sites, as it appears in Figure 4 the majority of users are aware of the listed risks. Risk perception rates such as viruses and spam exceed 90%. However, lower rates present risks such as phishing and identity theft that nevertheless still exceeds 50%. Which indicates that users are aware about risks in SNS.

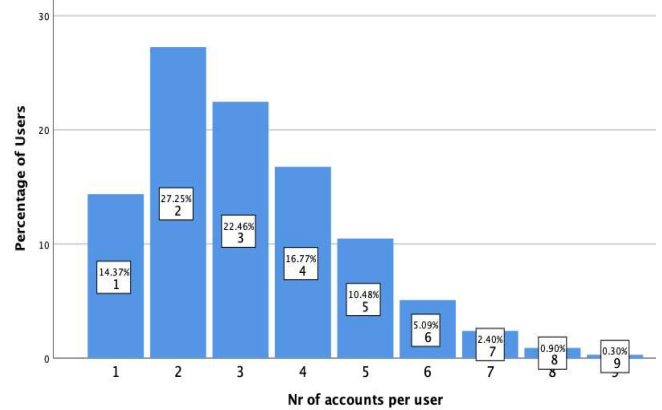


Fig. 3 Accounts per User

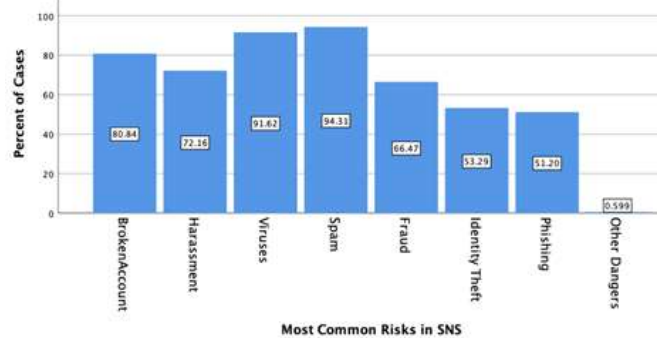


Fig. 4 Common Risks in SNSs

Regarding Exposure to Risk, details of participants' risk exposure are listed as it appears in Figure 5. The majority of participants appear to have been exposed to some risk, with the highest percentage (26.6%) having encountered at least 2 risks in their interaction participating in SNS's. The next higher rate of 21.3% is of that facing 3 different risks. The percentage that has never faced any risk at all is 11.7%.

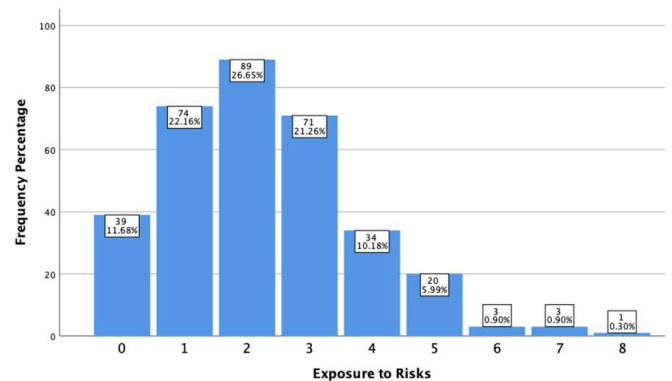


Fig. 5 Exposure to Risks

## V. CONCLUSION & FUTURE WORK

As for exposure to risk factors in Table 1, there is an analysis per factor and how both male and female behaves. It is observed that the averages between the two sexes are slightly different.

Regarding the results associated to 4th research question, the situation is as follows:

To examine the relationship behaviors in SNS and Demographic Characteristics of users the following zero hypothesis was stated and tested: Privacy Behavior and Age:  $H_0$ : There is no difference between different ages (of participating in SNS) regarding Privacy Behavior. Rejected. One-way ANOVA test was performed (excluding category 69+ as it was a constant in Normality test) ( $F [3,329] = 8,827$ ,  $p = 0.00$   $h^2 = 0.074$ ).

Perceived Control of Information & Education Level.  $H_0$ : There is no Difference between the Educational Level (of SNS users) regarding the Perceived Control of Information behavior. Rejected. One-way ANOVA test ( $F [2,331] = 3.529$ ,  $p = 0.030$   $n^2 = 0.020$ ) was performed.

Identity Information Disclosure and Age.  $H_0$ : There is no difference between the different age groups (of participating in SNS) regarding Identity Information Disclosure behavior. Rejected. One Way-ANOVA test (except for category 69+ as it was a constant in Normality test) was implemented ( $F [3,329] = 4,890$ ,  $p = 0.02$ ,  $h^2 = 0.042$ )

«I am concerned with the consequences of sharing identity information and gender  $H_0$ : There is no difference between Male & Female users in behavior “I am concerned with the consequences of sharing identity information” Rejected. Mann-Whitney  $t = 10642.50$ ,  $n_1 = 110$ ,  $n_2 = 224$ ,  $p < 0,05$ ).

“I believe that my identity information is well protected on the Internet” and Education Level.  $H_0$ : There is no difference between Educational Level (SNS Users) regarding “I believe that my identity information is well protected online”. Rejected. Kruskal-Wallis test ( $t = 7,543$ ,  $df = 2$ ,  $p = 0.023$ )

As for the rest of the results on relationships between behaviors and socio-demographic characteristics, it was found that Risk Taking, Trust in SNS Companies, & Privacy Concern do not relate to Gender, Age, and Educational Level.

Regarding the results associated to 5th research question, the situation is as follows:

To examine the relationship between Exposure to Risk in SNS and Socio-Demographic Characteristics of users the following zero hypothesis was stated and tested: Exposure to Risk and Gender  $H_0$ : There is no difference between 'Male' and 'Female' in Exposure to Risk in SNSs. Rejected. Mann-Whitney test ( $t = 9220.50$ ,  $n_1 = 110$ ,  $n_2 = 224$ ,  $p < 0.05$ )

As there was rejection of the Zero Hypothesis, we conclude that Exposure to Risk is Gender Related.

As for the rest of the results of relationships between Exposure to Risk and socio-demographic characteristics, it was found that Exposure to Risk do not relate to Age and Educational Level.

The enormous expansion of the Internet and Social Networks has worsened issues such as privacy and security. End-user risks relate to and target the personal information of the user, who himself (more often) intentionally than deliberately "publishes". It has been argued by researchers that most of the risks related to Information Technologies and Social Networks are related to Privacy. The safety issue of social networking users, either it concerns their personal data or other risks that they pose to users is a matter that is almost constantly a concern for users and researchers. As the use of Social Networking Sites grows relevant research become almost necessary and should be encouraged.

Concerning Greek Reality, the results of the present study cannot be compared with other similar studies as no other relevant studies have been identified. However, a study, carried out by Fogel & Nehmad (2009), [47], was identified, in which some measurements and results of the tested characteristics can be compared with the present study.

Limitation of the present study could be the issue of women's participation, as the sample of the female population is larger than that of men. Women, however, are supported by Kimbrough et al. (2013), [52], are more involved in social networking than men, which is also supported by other findings (Alnjadat et al., 2019, [53]), (Hargittai, 2007, [54]), (Madden & Zickuhr, 2011, [55]). Although this difference, according to recent US surveys, tends to be eliminated (Madden & Zickuhr, 2011, [55]), it has also been argued that women are involved in more research (Kimbrough et al., 2013), (Branley & Covey, 2018, [56]). Another limitation that could exist is that of under-representation of participants in the 69+ year age group. But as technology penetration at these ages is less likely, the relevant research may be a field for further research.

## REFERENCES

- [1] Clement, J. (2019, August 14). Number of social media users worldwide 2010-2021. Statista. <https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/>
- [2] Hilbert, M. (2016). Big Data for Development: A Review of Promises and Challenges. *Development Policy Review*, 34(1), 135–174. <https://doi.org/10.1111/dpr.12142>
- [3] Todd, H. K., Dave Gershgorn, Sarah. (2018, March 29). The Cambridge Analytica scandal is wildly confusing. This timeline will help. Quartz. <https://qz.com/1240039/the-cambridge-analytica-scandal-is-confusing-this-timeline-will-help/>
- [4] González-Bailón, S. (2018, April 4). Want to change Facebook? Don't delete your account—use it for good. Quartz. <https://qz.com/1244750/the-delete-facebook-movement-is-ultimately-self-defeating/>
- [5] Social Media and Our Privacy. (2016). *Futurism*. <https://vocal.media/futurism/social-media-and-our-privacy>
- [6] Today's social network sites: An analysis of emerging security risks and their counter measures. (2017). 2017 International Conference on Communication Technologies (ComTech), Communication Technologies (ComTech), 2017 International Conference On, 143. <https://doi.org/10.1109/COMTECH.2017.8065764>
- [7] Fire, M., Goldschmidt, R., & Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys Tutorials*, 16(4), 2019–2036. <https://doi.org/10.1109/COMST.2014.2321628>
- [8] Young, Kimberly S. (1996). INTERNET ADDICTION: THE EMERGENCE OF A NEW CLINICAL DISORDER. Vol. 1 No. 3.,

- [9] Lee, Y.-H., Ko, C.-H., & Chou, C. (2015). Re-visiting internet addiction among Taiwanese students: A cross-sectional comparison of students' expectations, online gaming, and online social interaction. *Journal Of Abnormal Child Psychology*, 43(3), 589–599. <https://doi.org/10.1007/s10802-014-9915-4>
- [10] Bányaí, F., Zsila, Á., Király, O., Maraz, A., Elekes, Z., Griffiths, M. D., Andreassen, C. S., & Demetrovics, Z. (2017). Problematic Social Media Use: Results from a Large-Scale Nationally Representative Adolescent Sample. *Plos One*, 12(1), e0169839–e0169839. <https://doi.org/10.1371/journal.pone.0169839>
- [11] Ponte, C., Simões, J. A., & Jorge, A. (2013). Do questions matter on children's answers about internet risk and safety? *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 7(1). <https://doi.org/10.5817/CP2013-1-2>
- [12] Ybarra, M. L., Mitchell, K. J., Wolak, J., & Finkelhor, D. (2006). Examining Characteristics and Associated Distress Related to Internet Harassment: Findings From the Second Youth Internet Safety Survey. *Pediatrics*, 118(4), e1169–e1177. <https://doi.org/10.1542/peds.2006-0815>
- [13] DeMarco, J. N., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M., Caretti, V., Schimmenti, A., & Bifulco, A. (2017). Digital Dangers and Cyber-Victimisation: A Study of European Adolescent Online Risky Behaviour for Sexual Exploitation. *Clinical Neuropsychiatry*, 14(1), 104–112.
- [14] Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer-Mediated Communication*, 15(1), 83–108. <https://doi.org/10.1111/j.1083-6101.2009.01494.x>
- [15] Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1), 153–160. <https://doi.org/10.1016/j.chb.2008.08.006>
- [16] Christofides, E., Muise, A., & Desmarais, S. (2012a). Hey Mom, What's on Your Facebook? Comparing Facebook Disclosure and Privacy in Adolescents and Adults. *Social Psychological and Personality Science*, 3. <https://doi.org/10.1177/1948550611408619>
- [17] Christofides, E., Muise, A., & Desmarais, S. (2012b). Risky Disclosures on Facebook: The Effect of Having a Bad Experience on Online Behavior. *Journal of Adolescent Research*, 27(6), 714–731. <https://doi.org/10.1177/0743558411432635>
- [18] Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook Users' Online Privacy Protection: Risk, Trust, Norm Focus Theory, and the Theory of Planned Behavior. *Journal of Social Psychology*, 154(4), 352–369. <https://doi.org/10.1080/00224545.2014.914881>
- [19] Kezer, M., Sevi, B., Cemalcilar, Z., & Baruh, L. (2016). Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology*, 10(1), 52–71. <https://doi.org/10.5817/CP2016-1-2>
- [20] Meter, D. J., & Bauman, S. (2015). When Sharing Is a Bad Idea: The Effects of Online Social Network Engagement and Sharing Passwords with Friends on Cyberbullying Involvement. *Cyberpsychology, Behavior And Social Networking*, 18(8), 437–442. <https://doi.org/10.1089/cyber.2015.0081>
- [21] Sampasa-Kanyinga, H., & Hamilton, H. A. (2015). Use of Social Networking Sites and Risk of Cyberbullying Victimization: A Population-Level Study of Adolescents. *Cyberpsychology, Behavior And Social Networking*, 18(12), 704–710. <https://doi.org/10.1089/cyber.2015.0145>
- [22] Mitchell, K. J., & Ybarra, M. (2009). Social networking sites: Finding a balance between their risks and benefits. *Archives Of Pediatrics & Adolescent Medicine*, 163(1), 87–89. <https://doi.org/10.1001/archpediatrics.2008.534>
- [23] Livingstone, S., & Brake, D. R. (2010). On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. *Children & Society*, 24(1), 75–83. <https://doi.org/10.1111/j.1099-0860.2009.00243.x>
- [24] Weir, G. R. S., Toolan, F., & Smeed, D. (2011). The threats of social networking: Old wine in new bottles? *Information Security Technical Report*, 16(2), 38–43. <https://doi.org/10.1016/j.istr.2011.09.008>
- [25] Hongyu Gao, Jun Hu, Tuo Huang, Jingnan Wang, & Yan Chen. (2011). Security Issues in Online Social Networks. *IEEE Internet Computing, Internet Computing, IEEE, IEEE Internet Comput.*, 4, 56. <https://doi.org/10.1109/MIC.2011.50>
- [26] Vandoninck, S., d'Haenens, L., De Cock, R., & Donoso, V. (2012). Social Networking Sites and Contact Risks among Flemish Youth. *Childhood: A Global Journal of Child Research*, 19(1), 69–85.
- [27] Ephraim, P. E. (2013). African youths and the dangers of social networking: A culture-centered approach to using social media. *Ethics & Information Technology*, 15(4), 275–284. <https://doi.org/10.1007/s10676-013-9333-2>
- [28] Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, 133(1), 111.
- [29] Montes-Vozmediano, M., García-Jiménez, A., & Menor-Sendra, J. (2018). Teen Videos on YouTube: Features and Digital Vulnerabilities. *Comunicar: Media Education Research Journal*, 26(54), 61–69.
- [30] Tsitsika, A., Critselis, E., Kormas, G., Filippopoulou, A., Tounissidou, D., Freskou, A., Spiliopoulou, T., Louizou, A., Konstantoulaki, E., & Kafetzis, D. (2009). Internet use and misuse: A multivariate regression analysis of the predictive factors of internet use among Greek adolescents. *European Journal Of Pediatrics*, 168(6), 655–665. <https://doi.org/10.1007/s00431-008-0811-1>
- [31] Frangos, C. C., Frangos, C. C., & Sotiropoulos, I. (2011). Problematic Internet Use Among Greek University Students: An Ordinal Logistic Regression with Risk Factors of Negative Psychological Beliefs, Pornographic Sites, and Online Games. *CyberPsychology, Behavior & Social Networking*, 14(1/2), 51–58. <https://doi.org/10.1089/cyber.2009.0306>
- [32] Kormas, G., Critselis, E., Janikian, M., Kafetzis, D., & Tsitsika, A. (2011). Risk factors and psychosocial characteristics of potential problematic and problematic internet use among adolescents: A cross-sectional study. *BMC Public Health*, 11, 595–595. <https://doi.org/10.1186/1471-2458-11-595>
- [33] Floros, G. D., Siomos, K. E., Fisoun, V., Dafouli, E., & Geroukalis, D. (2013). Adolescent online cyberbullying in Greece: The impact of parental online security practices, bonding, and online impulsiveness. *Journal of School Health*, 6, 445.
- [34] Antoniadou, N., & Kokkinos, C. M. (2015). A review of research on cyber-bullying in Greece. *International Journal of Adolescence and Youth*, 20(2), 185–201. <https://doi.org/10.1080/02673843.2013.778207>
- [35] Gkiomisi, A., Gkrizioti, M., Gkiomisi, A., Anastasilakis, D. A., & Kardaras, P. (2017). Cyberbullying Among Greek High School Adolescents. *Indian Journal Of Pediatrics*, 84(5), 364–368. <https://doi.org/10.1007/s12098-016-2256-2>
- [36] Giota, K. G., & Kleftharas, G. (2013). The role of personality and depression in problematic use of social networking sites in Greece. *Cyberpsychology*, 7(3), 1–10. <https://doi.org/10.5817/CP2013-3-6>
- [37] Kourouthanassis, P., Lekakos, G., & Gerakis, V. (2015). Should I stay or should I go? The moderating effect of self-image congruity and trust on social networking continued use. *Behaviour & Information Technology*, 34(2), 190–203. <https://doi.org/10.1080/0144929X.2014.948489>
- [38] Tsiolka, E., Bergiannaki, I. D., Margariti, M., Malliori, M., & Papageorgiou, C. (2017). Dysfunctional internet behaviour symptoms in association with personality traits. *Psychiatrike = Psychiatriki*, 28(3), 211–218. <https://doi.org/10.22365/jpsych.2017.283.211>
- [39] infographic-information-technologies-2019—ELSTAT. (n.d.). Retrieved November 22, 2019, from <https://www.statistics.gr/el/infographic-information-technologies-2019>
- [40] Greece in Numbers—ELSTAT. (n.d.). Retrieved November 22, 2019, from <https://www.statistics.gr/greece-in-figures>
- [41] Statistics- ELSTAT. (n.d.). Retrieved November 20, 2019, from <https://www.statistics.gr/el/statistics/-/publication/SAM07/>
- [42] Statistics. (n.d.). Cyberbullying Research Center. Retrieved May 31, 2018, from <https://cyberbullying.org/statistics>
- [43] Salourou, R. (2015, September 19). Ready to explode the demographic bomb, Kathimerini. <https://www.kathimerini.gr/831452/article/oikonomia/ellhnikh-oikonomia/etoimh-na-ekragei-h-dhmografikh-vomva>
- [44] Rosen, L. D., Whaling, K., Carrier, L. M., Cheever, N. A., & Rökkum, J. (2013). The Media and Technology Usage and Attitudes Scale: An empirical investigation. *Computers in Human Behavior*, 29(6), 2501–2511. <https://doi.org/10.1016/j.chb.2013.06.006>
- [45] Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. 3(1), 28.
- [46] Pan, Y., & Zinkhan, G. M. (2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, 82(4), 331–338. <https://doi.org/10.1016/j.jretai.2006.08.006>

## Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0

[https://creativecommons.org/licenses/by/4.0/deed.en\\_US](https://creativecommons.org/licenses/by/4.0/deed.en_US)

- [47] Fogel and Nehmad—2009—Internet social network communities Risk taking. .pdf. (n.d.).
- [48] Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157–165. <https://doi.org/10.1002/asi.20459>
- [49] Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents—Measurement validity and a regression model. *Behaviour & Information Technology*, 23(6), 413–422. <https://doi.org/10.1080/01449290410001715723>
- [50] Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109–125. <https://doi.org/10.1057/jit.2010.6>
- [51] Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. In *IDMAa and IMS Code Conference*, 3.
- [52] Kimbrough, A., Guadagno, R., & Janeann Dill, D. der P. (2013). Gender differences in mediated communication: Women connect more than do men. [https://www.academia.edu/19260090/Gender\\_differences\\_in\\_mediated\\_communication\\_Women\\_connect\\_more\\_than\\_do\\_men](https://www.academia.edu/19260090/Gender_differences_in_mediated_communication_Women_connect_more_than_do_men)
- [53] Alnjadat, R., Hmaid, M. M., Samha, T. E., Kilani, M. M., & Hasswan, A. M. (2019). Gender variations in social media usage and academic performance among the students of University of Sharjah. *Journal of Taibah University Medical Sciences*, 14(4), 390–394. <https://doi.org/10.1016/j.jtumed.2019.05.002>
- [54] Hargittai, E. (2007). Whose Space? Differences Among Users and Non-Users of Social Network Sites. *Journal of Computer-Mediated Communication*, 13(1), 276–297. <https://doi.org/10.1111/j.1083-6101.2007.00396.x>
- [55] Madden, M., & Zickuhr, K. (2011, August 26). 65% of online adults use social networking sites. Pew Research Center: Internet, Science & Tech. <https://www.pewresearch.org/internet/2011/08/26/65-of-online-adults-use-social-networking-sites/>
- [56] Branley, D. B., & Covey, J. (2018). Risky behavior via social media: The role of reasoned and social reactive pathways. *Computers in Human Behavior*, 78, 183–191. <https://doi.org/10.1016/j.chb.2017.09.036>

**Eleni Stratigopoulou** has completed (2019) the Master's program Social Information Systems of the Open University of Cyprus. Her main research interests include Cyber-bullying, Social Networks and threats' analysis in the World Wide Web.

**Prof. Klimis Ntalianis** received his diploma and Phd degrees both from the Electrical and Computer Engineering Department of the National Technical University of Athens (NTUA) in 1998 and 2003 respectively. From February 2020 he is a Professor at the West Attica University (Department of Marketing, Specialization: "Multimedia over the Internet"). Dr. Ntalianis has participated as editor in the proceedings of 3 International Conferences, he has written more than 150 scientific papers & deliverables and has received more than 1,000 citations. His main research interests include multimedia processing, social media analysis, crowdsourcing and data mining.

**Vasiliki Kikili** received her Bachelor and Master's degrees both from the Department of Music Studies of the National and Kapodistrian University of Athens in 2009 and 2014 respectively. Her main research interests include music analysis over Social Networks, pedagogical aspects of social networking and online education.

**Prof. Filotheos Ntalianis** is an Assistant Professor at the Department of Business Administration, University of Piraeus. He has completed his Ph.D. at Concordia University, Montreal, Canada and Graduate studies at Florida Atlantic University, Boca Raton, Florida, USA. He is an active researcher and his work has appeared in academic journals and conferences. His research interests focus on the areas of motivation, personality, psychological contracts, employee physical activity and health.