



## Online Social Networks: A Survey of Usage and Risks Experience among University Students in North-Central Nigeria

Victor Legbo Yisa<sup>1</sup>, Oluwafemi Osho<sup>2</sup>, and Isaac Soje

Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria

{<sup>1</sup>victor.yisa, <sup>2</sup>femi.osho}@futminna.edu.ng

**Abstract**—Online social networks (OSNs), since the advent of the first, have continued to influence virtually every facet of human existence, as well as appeal to users of different ages and races, including students. This study seeks to investigate the usage of online social networks and associated risks experienced among university students in North-Central, Nigeria. The study involves three tertiary institutions in North-Central Nigeria. Data were collected via questionnaires. Most of the respondents were male, full-time undergraduate students, and within the ages of 24 – 29. Findings reveal that most of the students use OSNs to interact with friends. More than half of the students usually uploaded their locations while online, actually connected with other users they did not know, have extended relationships that commenced online to offline relationship, and used most of their time on the networks for academic purposes. Other uses included dating and offering financial assistance to acquaintances. For most of the students, the use of OSNs had positively affected their performance. Most of the students were found to have experienced risks including identity theft, unsolicited and irrelevant messages, information-request attack, and stolen password attack.

**Keywords**—component; online social network; social networking site; security; risk; privacy

### I. INTRODUCTION

An Online social network, also called Social networking site (SNSs), can be defined as an online application that enable people to build a profile of themselves and share with users of which it is believed they have some connection. It can also be defined as an interactive website that interacts with you while giving you information. It is a group of applications based on the Internet that allows the generation and exchange of user-created contents [1]–[3]. Since the advent of the first OSN, SixDegrees.com [1], the networks have increased rapidly in number and sophistication. By 2010, up to 300 had pervaded the internet [4]. SNSs including Facebook, Instagram, 2go, Whatsapp, Twitter, and LinkedIn have intensely changed the way interaction is done on a global scale.

SNSs offer many advantages and usefulness. They can be used to increase sales, educate, meet new friends or old ones, and even as a tool to communicate with the general public [5]. They provide a platform for a user with no physical friend in the real world to have lots of friends on social media, without ever meeting them [5], [6]. A new complete

virtual community can be created where users irrespective of boundaries or other segregating values of traditional communities interact, socialize, do business, learn, and engage in a whole lot of other things. Disgruntled people in the physical world may enjoy a whole lot of happiness and acceptance on social media.

Social networking sites have had massive impact on people's online activities. Users update status or tweet about themselves [6], [7]. The number of those using social networking sites has more than doubled since 2008 [7] Facebook alone in 2016 has a total of 1.71 billion monthly active users [8], a figure greater than china's population which happens to be the world most populous country. Businesses, organizations and even governments have accepted the use of social networks in trying to achieve their aims.

With a population of over one hundred and eighty six million, Nigeria has an internet penetration level of 46.1 percent meaning over 86 million Nigerians have access to the internet [9]. Because of the proliferation of smart phones and internet services in the country, youngsters especially students are constantly on OSNs, updating status, chatting, dating, reading news, commenting on profiles or sharing multimedia information. Over the years, the use of OSNs amongst Nigerians has been increasing. Facebook alone boast of 16 million users as at February 2016.

In Nigeria, OSNs appeal not only to individuals; organizations, institutions and even government institutions now employ them. Students share educative materials, chat, make new friends, stream videos today using them. During the 2011 elections in the country, OSNs were actively engaged by politicians, who took their campaigns more often to the various SNSs where they could reach millions of Nigerians easily and directly [10].

However the many and diverse benefits that OSNs afford, like many systems, they are prone to be exploited for unethical uses. Unfortunately, many users can be said to be naïve regarding the security mechanisms of the networks. Thus, they become vulnerable to malicious users lurking behind their walls. A popular comedian was recently robbed after the wife had posted a picture of their recently acquired home on Instagram. There have been instances where OSNs were used as aid to commit criminal activities in the physical world. One example that readily comes to mind is the Cynthia Osokugu murder by some Facebook friends; an

event that shook the entire country in 2012. Investigations showed that she had made friends and given out chunks of personal information to her so called Facebook friends that killed her in a Lagos hotel after she had travelled to meet them [11]. These are clear examples of crimes that occurred due to users' ignorance and careless release of sensitive information on SNSs.

This study investigates the usage of online social networks and associated risks experienced among university students in North-Central, Nigeria.

The rest of the paper is organized as follows: a review of risks associated with online social networks and summary of related studies are presented in section II. Section III describes the methodology used in the survey. In section IV and V, the findings are presented and discussed respectively. Section VI concludes the study.

## II. LITERATURE REVIEW

### A. Online Social Networks Risks

Although the benefits of using social media abounds, it can also have serious security risks. While some of these risks are consequent of inherent vulnerabilities in SNSs, primarily, they are often caused or exacerbated by users themselves. Many users either lack basic knowledge to manage their security while online, or outrightly are care less about security. Consequently, attackers exploit these security lapses for economic, social, or psychological benefits [12].

Figure 1 presents a taxonomy of OSN risks. The risks are either IT- or Non-IT-related. Many studies have shown the evidence and effects of non-IT risks including excessive use [13], addiction [14], sexual solicitation and harassment [15], posting regret [16], [17].

On the other hand, IT-related risks on OSNs are basically privacy-related. Online privacy is a fundamental right of every OSN user. User typically expects to retain exclusive right over their information available online. Unfortunately, absolute privacy on SNSs is highly unlikely. Lucas and Borisov [18] opined that privacy breaches are inevitable, regardless of OSNs' proprietors' and users' efforts. These breaches are directly or indirectly caused by users themselves, proprietors of SNSs, and other malicious users.

Firstly, users, either intentionally or unintentionally, expose themselves to privacy risks. While users could unintentionally self-breach their privacy [18], many, however, often display nonchalant disposition to personal privacy. Studies have shown users' indifference to their privacy, leaving default security settings unchanged [19], and in some cases, despite being cognizant of the security implications [20]. Unfortunately, this is more common among young OSN users [1]. Adult users have been found to be more privacy-conscious while online [21], [22]. Self-breach of privacy exposes users to risks including over-disclosure of information and cyber-stalking.

Secondly, OSN proprietors also expose users to privacy risks. These networks naturally thrive on their capacity to provide easy-to-use functionalities that encourage information sharing. Unfortunately, security often suffers. This is because, it is almost impossible to guarantee simultaneously usability, functionality, and security. Many

of the OSNs only afford weak security mechanisms. Hence, they are prone to automatic crawling and access [18], [23]. Other risks center on proprietors' unethical use of users' personal information [24]. Users' data can be mined and sold for targeted advertisements [25].

Lastly, privacy breaches are caused by malicious users. Specifically, most risks are the handiwork of malicious users who often pose as legitimate users. Regrettably, these constitute a significant portion of OSN users. In a study by [26], it was discovered that up to 10% of profiles on Facebook were either fake or duplicate accounts. As a result, users are exposed to risks like spamming, social engineering, stalking, identity theft, phishing, and malware attacks [22], [27]–[30].

### B. Related works

The prevalent use of social media sites has attracted the interest of many researchers. Studies by [31], [32] focused on usage of SNS amongst students' of tertiary institutions. While [31] focused on a University in Zimbabwe, [32] considered one in Nsukka, Nigeria. Some studies have investigated the impact of social media on students' academic performance. These include [33] who focused on impact on students' performance in Ghana. The other study, by [34] considered students in Kosovo. Despite the different geographical location, the findings of [31], [32], [34] suggest that high percentage of tertiary institution students use SNS, among which Facebook is one of the most prevalent. Secondly, SNS usage has a huge impact on the academic performance of students.

Many authors have critically examined the security issues associated with the use of online social networks. These include privacy issues faced by users of social networking site [35], types of associated cyber threats [36], impact of provided user information on privacy [37], [38].

## III. METHODOLOGY

To achieve the objective of the study, a survey of students in three universities in the north central part of Nigeria was conducted. The schools were Federal University of Technology, Minna, and Ibrahim Badamasi Babangida University, Lapai, both in Niger State, and University of Abuja, in the Federal Capital Territory. The survey took place in 2014. Data were collected via questionnaires. A total of 300 were distributed, while 266 were returned. Out of the completed and returned questionnaires, 12 were found to be invalid. The remaining 254 were consequently used for analysis. Most of the respondents were male, 64.6% v. 35.4%; full-time undergraduate students, 79.5%; within the ages of 24 – 29, 46.1%; and used Facebook, 35.8%. The demographic characteristics of the respondents are presented in Table I.

The questionnaire sought information on respondents' usage of online social networks, effects of and risks experienced with the usage. The 5-point Likert-type was used to indicate level of agreement. It consisted of SA = Strongly Agree, A = Agree, N = Neutral, D = Disagree, and SD = Strongly Disagree.

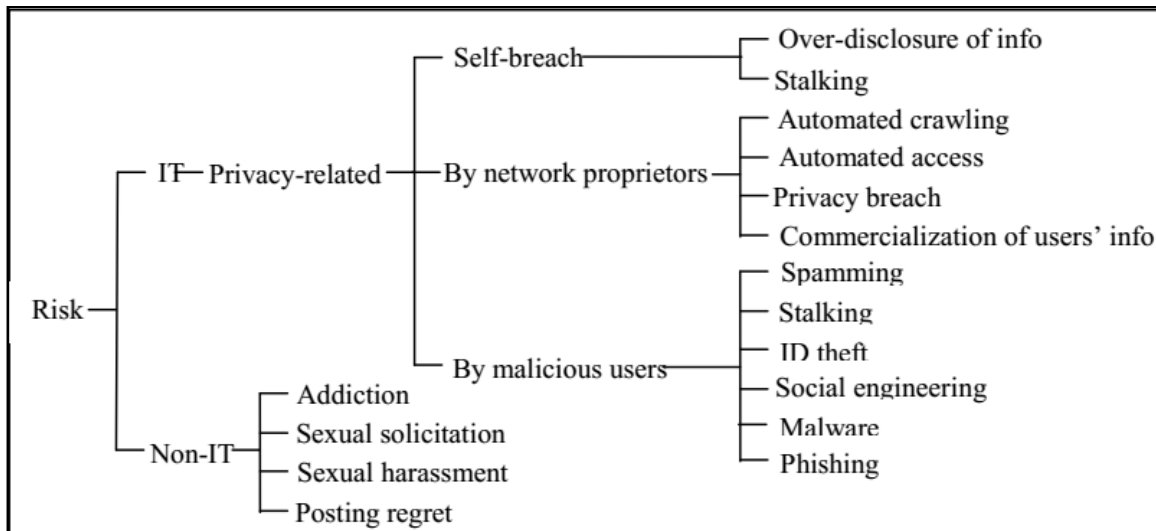


Figure 1. Taxonomy of OSN risks

TABLE I. RESPONDENTS' DEMOGRAPHIC CHARACTERISTICS

	Freq	%
<b>Sex</b>		
Male	164	64.6
Female	90	35.4
Total	254	100.0
<b>Studentship type</b>		
Undergraduate (part-time)	20	7.9
Undergraduate (full-time)	202	79.5
Postgraduate (part-time)	10	3.9
Postgraduate (full-time)	22	8.7
Total	254	100.0
<b>Age</b>		
18 – 23	101	39.8
24 – 29	117	46.1
30 – 35	27	10.6
> 35	9	3.5
Total	254	100.0
<b>Online social network used</b>		
Facebook	91	35.8
Google+	11	4.3
Whatsapp	62	24.4
Twitter	14	5.5
2GO	29	11.4
Instagram	8	3.1
EBuddy	5	2.0
Badoo	8	3.1
BBM Chat	21	8.3
Yahoo Messenger	5	2.0
Total	254	100.0

#### IV. RESULTS

##### A. Use of Online Social Networks and Effects on Academics

From our findings, as presented in Table II, almost all the university students, 93.3%, used online social network to interact with other users. More than half of the students usually uploaded their locations while online (66.9%),

actually connected with other users they did not know (70.1%), have extended relationships that commenced online to offline relationship (61.0%), and used most of their time on the networks for academic purposes (55.1%). In the same vein, compared to those who have not, more students have dated someone met on the social networks (47.6%). However, fewer students (31.9%) reported they have sent money to their online acquaintance. On the other hand, 53.5% confessed they had offered financial help to friends on their social networks.

On the effect of online social network use on academic performance, more than half of the students, 57.5%, either agreed or strongly agreed the use had positively affected their performance.

##### B. Risks Associated with Use of Online Social Networks

Table II also contains findings on risks experienced by students on online social networks. With the exception of physical threat or assault (39.7%<sup>s</sup>), most of the students reported having experienced all identified risks. These risks include identity theft (51.9%), unsolicited and irrelevant messages (81.5%), information-request attack (75.9%), and stolen password attack (66.9%).

#### V. DISCUSSION

The study sought to identify the different uses of online social networks by university students, the effect of the use on their academics, and security risks they are exposed to while online. Students from three universities were surveyed. Findings revealed that in addition to using online social networks for academic purposes, university students also use online social networks for other purposes, including meeting new acquaintances and even dating. Many were found to have extended relationships that commenced online offline. Evidently, this category of online social networks users feel very much at ease while online. They tend to develop and maintain relationships without much anxiety. These findings agree with those of [14] and [39].

TABLE II. USAGE OF SOCIAL NETWORK, EFFECTS OF USAGE ON ACADEMICS AND RISKS EXPERIENCED ON THE NETWORKS

	SA (%)	A (%)	N (%)	D (%)	SD (%)
<b>Usage</b>					
I interact with friends on social media sites	162 (63.8)	75 (29.5)	4 (1.6)	6 (2.4)	7 (2.8)
I have friends I interact with that I don't know	101 (39.8)	77 (30.3)	14 (5.5)	28 (11.0)	34 (13.4)
I upload my location when I chat or upload a status	63 (24.8)	107 (42.1)	33 (13.0)	26 (10.2)	25 (9.8)
I have met physically with friends met on social media sites	73 (28.7)	82 (32.3)	18 (7.1)	48 (18.9)	33 (13.0)
I have sent money to friends on social media sites	28 (11.0)	53 (20.9)	37 (14.6)	58 (22.8)	78 (30.7)
I have met and dated someone via social media sites	57 (22.4)	64 (25.2)	34 (13.4)	52 (20.5)	47 (18.5)
I use most of my time on social media for academic purposes	68 (26.8)	72 (28.3)	49 (19.3)	36 (14.2)	29 (11.4)
<b>Effects of usage on academics</b>					
My usage of social media sites has affected my academic performance in a positive way	75 (29.5)	71 (28.0)	38 (15.0)	34 (13.4)	36 (14.2)
<b>Usage risks</b>					
I have been physically threatened or assaulted by any of my friends from these social networking sites	40 (15.7)	61 (24.0)	41 (16.1)	51 (20.1)	61 (24.0)
I have experienced some identity theft online (i.e. someone posing as you on the net with your correct details)	57 (22.4)	75 (29.5)	50 (19.7)	42 (16.5)	30 (11.8)
I have received unsolicited and irrelevant messages on my social media account	93 (36.6)	114 (44.9)	27 (10.6)	11 (4.3)	9 (3.5)
Someone sent me a message on social networking sites requesting for my confidential details	72 (28.3)	121 (47.6)	29 (11.4)	20 (7.9)	12 (4.7)
I have experienced inability to log into any social networking sites due to my password being no longer correct	58 (22.8)	112 (44.1)	43 (16.9)	23 (9.1)	18 (7.1)

However, many students seemed to care less about their security. The online networks may have become so natural an ambience that many use them without consideration for their privacy and security. For instance, most of the students reveal locations while online. This has been referred to as unintentional self-breach of privacy [18]. Findings also revealed most of the students having connections they were actually not familiar with. These confirm findings in previous studies that categorized young users of online social networks as indifferent about protecting their privacy [1]. One reason suggested is their ignorance or limited knowledge of the public nature of the internet.

Considering their seeming lackadaisical attitude to security, it was not surprising to that most of the students have experienced one form of attack or the other while using their online social networks. Our findings confirm existing findings that identified social media sites as a veritable platform where different attacks, including spamming [23], identity theft [22], information-request – with the intent of launching a phishing attack [28], and assault [39], are targeted at users.

The success of most of these attacks depends to a large extent on the type and quantity of information that users share online, which is a direct consequence of the level of importance they attach to their privacy and security. Consequently, the need to be more circumspect while online cannot be overemphasized.

## VI. CONCLUSION

This study has increased our understanding of the acceptance of online social networks by students of universities in North-Central Nigeria who use them not only for academic purpose, but also to develop and maintain social relationships. On the other hand, they too, like other users, are not spared by malicious users who inundate them with unsolicited and irrelevant messages, and launch other attacks to steal their online credentials and identity.

Consequently, the need for the students to be more security aware while using these networks cannot be over-emphasized.

## REFERENCES

- [1] D. M. Boyd and N. B. Ellison, "Social Network Sites: Definition, History, and Scholarship Social Network Sites: A Definition," *J. Comput. Commun.*, vol. 13, no. 1, pp. 210–230, 2007.
- [2] C. Steinfield, N. B. Ellison, C. Lampe, and J. Vitak, "Online social network sites and the concept of social capital," *Front. New Media Res.*, pp. 115–131, 2012.
- [3] A. Ahmad, "A Short Description of Social Networking Websites And Its Uses," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 2, pp. 124–128, 2011.
- [4] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and Security for Online Social Networks: Challenges and Opportunities," *IEEE Netw.*, vol. 24, no. 4, pp. 13–18, 2010.
- [5] P. Collin, K. Rahilly, I. Richardson, and A. Third, "The Benefits of Social Networking Services," 2011.
- [6] R. Sawyer, "The Impact of New Social Media on Intercultural Adaptation," University of Rhode Island, 2011.
- [7] K. N. Hampton, L. S. Goulet, L. Rainie, and K. Purcell, "Social networking sites and our lives," 2011.
- [8] Statista, "Number of monthly active Facebook users worldwide as of 2nd quarter 2016 (in millions)." [Online]. Available: <http://www.statista.com/statistics/263424/the-largest-energy-utility-companies-worldwide-based-on-market-value/>.
- [9] Internet Live Stats, "Nigeria Internet Users." [Online]. Available: <http://www.internetlivestats.com/internet-users/nigeria/>.
- [10] N. Okoro and K. A. Nwafo, "Social Media and Political Participation in Nigeria during the 2011 General Elections: The Lapses and the Lessons," *Glob. J. Arts, Humanit. Soc. Sci.*, vol. 1, no. 3, pp. 29–45, 2013.
- [11] E. Usman, "How ex-General's daughter, Cynthia, was killed by facebook 'friends,'" *Vanguard Newspaper*, 2012.
- [12] A. Larionovs, A. Teilans, and P. Grabusts, "CORAS for Threat and Risk Modeling in Social Networks," *Procedia Comput. Sci.*, vol. 43, pp. 26–32, 2015.
- [13] C. M. K. Cheung, P.-Y. Chiu, and M. K. O. Lee, "Online social networks: Why do students use facebook?," *Comput. Human Behav.*, vol. 27, pp. 1337–1343, 2011.

- [14] L. W. Vilca and M. Vallejos, "Computers in Human Behavior Construction of the Risk of Addiction to Social Networks Scale ( C r . A . R . S . )," *Comput. Human Behav.*, vol. 48, pp. 190–198, 2015.
- [15] M. L. Ybarra and K. J. Mitchell, "How Risky are Social Network Sites? A Comparison of Places Online Where Youth Sexual Solicitation and Harassment Occurs," *Pediatrics*, vol. 121, no. 2, pp. e350–e357, 2010.
- [16] W. Xie and C. Kang, "See you, see me: Teenagers' self-disclosure and regret of posting on social network site," *Comput. Human Behav.*, vol. 52, pp. 398–407, 2015.
- [17] Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "I regretted the minute I pressed share: A qualitative study of regrets on Facebook," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, 2011, p. 10.
- [18] M. M. Lucas and N. Borisov, "flyByNight: Mitigating the Privacy Risks of Social Networking," in *Proceedings of the 7th ACM workshop on Privacy in the electronic society*, 2008, pp. 1–8.
- [19] R. Gross and A. Acquisti, "Information Revelation and Privacy in Online Social Networks (The Facebook case)," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, 2005, pp. 71–80.
- [20] J. L. Becker and H. Chen, "Measuring privacy risk in online social networks," in *Proceedings of the 2009 Workshop on Web (Vol. 2)*, 2009.
- [21] N. Li and G. Chen, "Sharing Location in Online Social Networks," *IEEE Netw.*, vol. 24, no. 5, pp. 20–25, 2010.
- [22] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," *Comput. Human Behav.*, vol. 26, pp. 406–418, 2010.
- [23] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks," in *Proceedings of the 18th international conference on World Wide Web*, 2009, pp. 551–560.
- [24] G. Cecere, F. Le Guel, and N. Soulie, "Perceived internet privacy concerns on social networks in Europe," *Technol. Forecast. Soc. Change*, vol. 96, pp. 277–287, 2015.
- [25] C. Patsakis, A. Zigoritos, and A. Papageorgiou, "Distributing privacy policy over multimedia content across multiple online social networks," *Comput. Networks*, vol. 75, pp. 531–543, 2014.
- [26] A. Vishwanath, "Habitual Facebook Use and its Impact on Getting Deceived on Social Media," *J. Comput. Commun.*, vol. 20, no. 1, pp. 83–98, 2015.
- [27] G. Brown, T. Howe, M. Ihbe, A. Prakash, and K. Borders, "Social networks and context-aware spam," in *Proceedings of the 2008 ACM conference on Computer supported cooperative work*, 2008, pp. 403–412.
- [28] T. Jagatic, N. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing \*," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, 2007.
- [29] G. Yan, G. Ghen, S. Eidenbenz, and N. Li, "Malware Propagation in Online Social Networks: Nature, Dynamics, and Defense Implications," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, 2011, pp. 196–206.
- [30] X. Zheng, Z. Zeng, Z. Chen, Y. Yu, and C. Rong, "Detecting spammers on social networks," *Neurocomputing*, vol. 159, pp. 27–34, 2015.
- [31] D. Christina, N. Fanuel, and M. Stella, "The use of social media technology in universities: A case of Solusi University, Zimbabwe," *J. Media Commun. Stud.*, vol. 7, no. 5, pp. 101–111, 2015.
- [32] C. O. Omekwu, H. N. Eke, and N. J. Odoh, "The Use of Social Networking Sites among the Undergraduate Students of University of Nigeria, Nsukka," *Libr. Philos. Pract.*, pp. 1–26, 2014.
- [33] M. Owusu-Acheaw and A. G. Larson, "Use of Social Media and its Impact on Academic Performance of Tertiary Institution Students: A Study of Students of Koforidua Polytechnic, Ghana," *J. Educ. Pract.*, vol. 6, no. 6, pp. 94–101, 2015.
- [34] G. Beqiri, "The Impact of Social Media on Higher Education in Kosovo: The Student's Perspective," *Acad. J. Interdiscip. Stud.*, vol. 3, no. 2, pp. 155–164, 2014.
- [35] S. M. Abdulhamid, S. Ahmad, V. O. Waziri, and F. N. Jibril, "Privacy and National Security Issues in Social Networks: The Challenges," *Int. J. Comput. Internet Manag.*, vol. 19, no. 3, pp. 14–20, 2011.
- [36] W. Gharibi and M. Shaabi, "Cyber Threats In Social Networking Websites," *Int. J. Distrib. Parallel Syst.*, vol. 3, no. 1, pp. 119–126, 2012.
- [37] S. M. Abdulhamid, H. T. Abdulazeez, O. Abraham, and U. Mohammed, "Analyzing Membership Profile Privacy Issues in Online Social Networks," *IUP J. Inf. Technol.*, vol. 7, no. 3, pp. 32–44, 2011.
- [38] S. Gangopadhyay and D. Dhar, "Social networking sites and privacy issues concerning youths," *Glob. Media J. - Indian Ed.*, vol. 5, no. 1, pp. 1–7, 2014.
- [39] V. Sánchez, N. Muñoz-fernández, and R. Ortega-ruíz, "Computers in Human Behavior "Cyberdating Q \_ A": An instrument to assess the quality of adolescent dating relationships in social networks," *Comput. Human Behav.*, vol. 48, pp. 78–86, 2015.