



## ENhancing seCurity and privAcy in the Social wEb: a user-centered approach for the protection of minors



### WP3 - Human and societal aspects of security and privacy in the social web Deliverable D3.1 "Report on user and societal aspects, and on usability of security and privacy OSN systems"

<b>Editor(s):</b>	Panagiotis Zaphiris (CUT)
<b>Author(s):</b>	Andreas Polydorou (CUT), Antigoni Parmaxi (CUT), Antonia Gogoglou (AUTH), Vaia Moustaka (AUTH), Tristan Caulfield (UCL), Athanasios Lekkas (INNO), Marios Vodas (LST)
<b>Dissemination Level:</b>	Public
<b>Nature:</b>	Report
<b>Version:</b>	0.8










#### PROPRIETARY RIGHTS STATEMENT

This document contains information, which is proprietary to the ENCASE Consortium. Neither this document nor the information contained herein shall be used, duplicated or communicated by any means to any third party, in whole or in parts, except with prior written consent of the ENCASE consortium.

ENCASE Project Profile

Contract Number	691025
Acronym	ENCASE
Title	ENhancing seCurity and privacy in the Social wEb: a user-centered approach for the protection of minors
Start Date	Jan 1 <sup>st</sup> , 2016
Duration	48 Months

Partners

	Cyprus University of Technology	Cyprus
	Telefonica Investigacion Y Desarrollo SA	Spain
	University College London	United Kingdom
	Cyprus Research and Innovation Center, Ltd	Cyprus
	SignalGenerix Ltd	Cyprus
	Aristotle University	Greece
	Innovators, AE	Greece
	Universita Degli Studi, Roma Tre	Italy
	LSTech Ltd	United Kingdom

### Document History

#### AUTHORS

(CUT) Panayiotis Zaphiris, Andreas Polydorou, Antigoni Parmaxi  
 (UCL) Tristan Caulfield  
 (AUTH) Antonia Gogoglou, Vaia Moustaka  
 (INNO) Athanasios Lekkas  
 (LST) Marios Vodas

#### VERSIONS

Version	Date	Author	Remarks
0.1	10.07.2017	CUT	Initial Table of Contents
0.2	16.08.2017	CUT,UCL	Added Literature Review
0.3	30.08.2017	CUT, LST, INNO	Added Methodology
0.4	05.10.2017	CUT	Added Survey Results & Discussion
0.5	30.11.2017	CUT, AUTH	Complete Literature Review
0.6	19.12.2017	CUT	Added Eye Tracker Studies
0.7	27.12.2017	CUT	Final editing and restructuring
0.8	30.12.2017	CUT	Final version

## Executive Summary

The overall aim of ENCASE is to leverage recent advancements in the field of usable security and privacy in order to design and implement a browser-based user-centric architecture for the protection of minors from malicious actors in online social networks. This architecture comprises three distinct browser-add-ons [1].

This deliverable, D3.1 “Report on user and societal aspects, and on usability of security and privacy OSN systems”, refers to the activities that were carried out as part of task 3.1 and task 3.2 of the work package 3 (WP3) of the ENCASE project. The purpose of task 3.1 was to identify the user requirements for security and privacy in Online Social Networks (OSNs). The purpose of task 3.2 was to study ways to improve user experience and user behavior when faced with security and privacy risks. The usability and user-experience of existing security and privacy systems for OSNs has been evaluated using query based techniques (questionnaires, interviews, focus groups) and through usability studies (observations, eye-tracking studies).

These requirements will be taken into consideration later in the project for the design guidelines and requirements of the ENCASE browser-add-ons. In line with the goals of ENCASE we carried out this task through a User-Centered Design approach.

To complete these tasks six studies were conducted, three in the form of meta-reviews of existing literature and three in the form of experimental studies. More specifically the following six studies were conducted:

1. “User behavior and experience when faced with security and privacy risks on OSN” (study 1) is an extensive literature review on user behavior and experience when faced with security and privacy risks on OSN.
2. “Meta-review on Cyberbullying” (study 2) is an extensive literature review that focuses on user behavior during this important and common online privacy and security issue.
3. “E-safety in Web 2.0 Learning Environments” (study 3) is a study where we explored the research and development pertaining to safety and security in Web 2.0 learning environments, as well as a review of web-based tools and applications that attempt to address security and privacy issues in OSNs.
4. “Discovering social bridges in Microblogs” (study 4) where we study the topology of a graph towards detecting the so called “social bridges”, i.e. the major supporters of malicious users, who have links and ties to both honest and malicious user communities.
5. “Survey of use of OSNs by minors” (study 5) is a work where we report the results of a survey run in Greece, Cyprus, and UK investigating the perceptions and concerns of minor users of OSNs in relation to online security and privacy. The participants were 76 teenagers (ages 12-17), users of OSNs.
6. “Usability evaluation of fraud detection systems” (study 6) is a work where we evaluated selected software in terms of usability by analyzing user comments and eye tracking technology. The participants in this study were parents who interacted with the selected software/add-ons and were then asked to rate each software.

As a result of our effort in D3.1, the following papers have been published:

1. Gogoglou, A., Theodosiou, Z., Kounoudes, T., Vakali, A., & Manolopoulos, Y. (2016, December). Early malicious activity discovery in microblogs by social bridges detection. In Signal Processing and Information Technology (ISSPIT), 2016 IEEE International Symposium on (pp. 132-137). IEEE. [106].
2. Parmaxi, A., Papadamou, K., Sirivianos, M., & Stamatelatos, M. (2017, July). E-safety in Web 2.0 Learning Environments: A Research Synthesis and Implications for Researchers and Practitioners. In International Conference on Learning and Collaboration Technologies (pp. 249-261). Springer, Cham. [81].
3. Ioannou, A., Blackburn J., Stringhini, G., De Cristofaro, E., Kourtellis N., Sirivianos, M., Zaphiris, P. (2017). From Risk Factors to Detection and Intervention: A Metareview and Practical Proposal for Research on Cyberbullying, in IST-Africa 2017 [71].

This report starts with a Literature Review for the subject of the study including the definitions and meanings of Usability, Security and Privacy on OSNs, Sensitive Content and the description of User Centred Design. Then it continues with the description and results of the six aforementioned studies.

## Table of Contents

Executive Summary.....	4
List of Figures .....	8
List of Tables .....	9
1. Introduction .....	10
2. Literature Review .....	12
2.1. Usability .....	12
2.2. Security and Privacy on OSNs .....	13
2.2.1 Sensitive Information.....	14
3. User Behavior and Experience when Faced with Security and Privacy Risks on OSN (study 1) ...	17
3.1. User behavior on OSN.....	17
3.2. Risks, threats, attacks and privacy leakage on OSN.....	17
3.3. Users behavior when faced privacy risks on OSN.....	18
4. Meta-review on Cyberbullying (study 2) .....	19
4.1. What is Cyberbullying .....	19
4.2. Methodology.....	19
4.3. Results.....	19
5. E-safety in Web 2.0 Learning Environments (study 3).....	23
5.1. Methodology.....	24
5.2. Findings .....	25
5.2.1 Parents’ and Teachers’ Attitudes and Experiences Towards E-safety in OSNs.....	26
5.2.2. E-safety Actions, Practices and Policies in OSNs.....	26
5.2.3. Evaluation of Schools’ E-safety Regulations in OSNs .....	27
5.2.4. Internet Safety Education .....	28
5.2.5. Implications for Researchers and Practitioners .....	28
5.3. Conclusions .....	29
5.4. Subsection References.....	30
6. Discovering Social Bridges in Microblogs (study 4).....	32
6.1. Social Bridges Detection: .....	33
7. Survey of use of OSNs by minors (study 5) .....	37
7.1. Study of previous research with similar surveys.....	37
7.2. Survey Design.....	37
7.3. Participants .....	37
7.4. Data Collection.....	37
7.5. Survey Results .....	38
7.6. Discussion on Findings .....	53
8. Usability Evaluation of Fraud Detection Systems (study 6) .....	55
8.1. Existing Security and Fraud Detection Systems .....	55
8.2. Methodology.....	56
8.3. Eye tracking studies .....	58
8.4. Results.....	59
8.4.1. Ex-ante questionnaire analysis results.....	59

8.4.2. Software & Add-ons evaluation results .....	60
9. Discussion / Conclusion.....	64
10. Appendices.....	65
10.1. Appendix 1: The Questionnaire used in the study.....	65
11. References .....	75

## List of Figures

Figure 1. Threats to online social network users [15].....	15
Figure 2. Flow diagram of the methodology adopted for exploring scholarly activity in e-safety in online collaborative environments.....	24
Figure 3. Overview of e-safety in Web 2.0 learning environments as derived from the e-safety corpus .....	25
Figure 4. A subsamplpe of Twitter user graph including the followers of spammers (SF) and the SF's followers. Three different components are identified depicted in black, red and green .....	34
Figure 5. Bar chart of the percentage differeces for the 6 networks features amongst the 3 identified user groups .....	35
Figure 6. A subset of Twitter user graph including a set of spammer users (isolated nodes) and the users they follow, excluding social bridges. The major connected component is depicted in the center.....	36
Figure 7. Age distribution of participants .....	38
Figure 8. Results diagram for Ques. 1, from survey Part A:.....	38
Figure 9. Results diagram for Ques. 2, from survey Part A:.....	38
Figure 10. Results Diagram for Ques. 3, from survey Part A: .....	39
Figure 11. Results Diagram for Ques. 4, from survey Part A: .....	39
Figure 12. Results Diagram for Ques. 5, from survey Part A: .....	39
Figure 13. Results Diagram for Ques. 2, from survey Part B:.....	40
Figure 14. Results Diagram for Ques. 3, from survey Part B:.....	40
Figure 15. Results Diagram for Ques. 4, from survey Part B:.....	40
Figure 16. Results Diagram for Ques. 5, from survey Part B:.....	41
Figure 17. Results Diagram for Ques. 6, from survey Part B:.....	41
Figure 18. Results Diagram for Ques. 7, from survey Part B:.....	41
Figure 19. Results Diagram for Ques. 8, from survey Part B:.....	42
Figure 20. Results Diagram for Ques. 9, from survey Part B:.....	42
Figure 21. Results Diagram for Ques. 10, from survey Part B: .....	42
Figure 22. Results Diagram for Ques. 11, from survey Part B: .....	43
Figure 23. Results Diagram for Ques. 12, from survey Part B.....	43
Figure 24. Results Diagram for Ques. 13, from survey Part B: .....	43
Figure 25. Results Diagram for Ques. 14, from survey Part B: .....	44
Figure 26. Results Diagram for Ques. 15, from survey Part B: .....	44
Figure 27. Results Diagram for Ques. 16, from survey Part B: .....	44
Figure 28. Results Diagram for Ques. 17, from survey Part B: .....	45
Figure 29. Results Diagram for Ques. 18, from survey Part B: .....	45
Figure 30. Results Diagram for Ques. 21, from survey Part B: .....	46
Figure 31. Results Diagram for Ques. 19, from survey Part B: .....	46
Figure 32. Results Diagram for Ques. 20, from survey Part B: .....	47
Figure 33. Results Diagram for Ques. 22, from survey Part B: .....	47
Figure 34. Results Diagram for Ques. 23, from survey Part B: .....	47



Figure 35. Results Diagram for Ques. 24(a), from survey Part B: .....	48
Figure 36. Results Diagram for Ques. 24(b), from survey Part B: .....	48
Figure 37. Results Diagram for Ques. 24(c), from survey Part B: .....	48
Figure 38. Results Diagram for Ques. 24(d), from survey Part B: .....	49
Figure 39. Results Diagram for Ques. 24(e), from survey Part B: .....	49
Figure 40. Results Diagram for Ques. 25, from survey Part B: .....	50
Figure 41. Results Diagram for Ques. 26, from survey Part B: .....	50
Figure 42. Results Diagram for Ques. 27, from survey Part B: .....	50
Figure 43. Results Diagram for Ques. 28, from survey Part B: .....	51
Figure 44. Results Diagram for Ques. 1, from survey Part C:.....	51
Figure 45. Results Diagram for Ques. 2, from survey Part C:.....	51
Figure 46. Results Diagram for Ques. 3, from survey Part C:.....	52
Figure 47. Results Diagram for Ques. 4(a), from survey Part C: .....	52
Figure 48. Results Diagram for Ques. 4(b), from survey Part C: .....	52
Figure 49. Results Diagram for Ques. 5, from survey Part C:.....	53
Figure 50. Answers form the Quest. "If your children have access to the internet how many hours they use it per day?" .....	59
Figure 51. Answers on the Quest. "Do you check where exactly your children surf on the Internet?" .....	60
Figure 52. Answers on the Quest. "Did you see anytime, that your children were at an inappropriate .....	60
Figure 53. Answers on the Quest. "Do you use any program or software that monitors your childrens' .....	60
Figure 54. Installation page.....	61
Figure 55. Import children .....	61
Figure 56. Choose categories of content to be blocked .....	62
Figure 57. Notification that website is blocked (Facebook) .....	62
Figure 58. Variety of keywords that are banned .....	63

## List of Tables

Table 1. Table of average rating score per parameter for each software .....	63
--	----

## 1. Introduction

The overarching technical goal of the ENCASE project is to provide end-users of the social web with tools that safeguard their privacy and their security (virtual and physical). The ENCASE project follows a user-centred design (UCD) approach in design and development of the browser add-ons. The research in these tasks (T3.1, T3.2), in combination with the upcoming tasks (T3.3) will lead to the development of design guidelines for the design of such systems (T3.4). T3.1 objective is to understand user’s expectations, needs and concerns with regards to usability, security and privacy of sensitive OSN content. T3.2 objective is to study user experience and user behaviour when faced with security and privacy risks.

To meet the objectives of these tasks the following work was conducted and reported in this deliverable:

1. “User behavior and experience when faced with security and privacy risks on OSN” (study 1): an extensive literature review on user behavior and experience when faced with security and privacy risks on OSN was carried out.
2. “Meta-review on Cyberbullying” (study 2): is an extensive literature review that looks at user behavior when faced with this important and common online privacy and security issue.
3. “E-safety in Web 2.0 Learning Environments” (study 3): is a work where we explore research works regarding the safety and security in Web 2.0 learning environments, as well as a review of web-based tools and applications that attempt to address security and privacy issues in Online Social Networks.
4. “Discovering social bridges in Microblogs” (study 4): is a work where we study the topology of a graph towards detecting “social bridges”, which are the links and ties to both honest and malicious user communities.
5. “Survey of use of OSNs by minors” (study 5): is a report with the results of a survey run in Greece, Cyprus and UK investigating the perceptions and concerns of minor users of OSNs regarding online security and privacy.
6. “Usability evaluation of fraud detection systems” (study 6): is a work where we evaluate several software solutions in terms of usability through the analysis of online comments and eye tracking technology.

Our effort on the aforementioned six studies resulted in the following publications:

1. Gogoglou, A., Theodosiou, Z., Kounoudes, T., Vakali, A., & Manolopoulos, Y. (2016, December). Early malicious activity discovery in microblogs by social bridges detection. In Signal Processing and Information Technology (ISSPIT), 2016 IEEE International Symposium on (pp. 132-137). IEEE. [106].
2. Parmaxi, A., Papadamou, K., Sirivianos, M., & Stamatelatos, M. (2017, July). E-safety in Web 2.0 Learning Environments: A Research Synthesis and Implications for Researchers and Practitioners. In International Conference on Learning and Collaboration Technologies (pp. 249-261). Springer, Cham. [81].

3. Ioannou, A., Blackburn J., Stringhini, G., De Cristofaro, E., Kourtellis N., Sirivianos, M., Zaphiris, P. (2017). From Risk Factors to Detection and Intervention: A Metareview and Practical Proposal for Research on Cyberbullying, in IST-Africa 2017 [71].

The remainder of this deliverable is structured as follows: In Section 2, we report the relevant literature review. Sections 3-8 are dedicated to the studies that we undertook during Tasks 3.1 and 3.2. Finally, we conclude in Section 9.

## 2. Literature Review

Usability, security, and privacy are three different concepts that were studied extensively by many researchers worldwide over the past few years. This section provides a clarification of the definitions and meanings of these key factors that are underlying this study. Moreover, sub-sections focus on the dangers in OSNs, on the security and privacy risks and cyberbullying.

### 2.1. Usability

The International Organization for Standardization (ISO) defines usability as "the extent to which a user can use a product to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context" (ISO 9241-11) [2]. Usability meaning, in other words, is "how well and how easily a user, without formal training can interact with an information system of a website" [3]. Like many other multimedia systems, websites and online platforms such as online social network can be assessed in terms of their usability.

Web evaluation used to test a web page the way it performs. Standard factors to be considered, while a website is analysed, are the way the data is organised and provided, and how a user can navigate the system and complete his 'task' [4].

Inside the context of a website usability does not cover only user interface issues, it also includes the content or the website, and the features that one system could perform. Bad web design will drive user away and give negative reputation to the company, organisation or network, etc [5].

Nowadays there are many definitions of the term usability and Human Computer Interaction (HCI). Human-Computer Interaction (HCI) is about designing computer systems that support people so that they can execute specific activities productively and safely. In HCI language, usability is more focused on creating a usable user interface or in other words to make a system easy to learn and easy to use [6]. In HCI field, usability is defined by the International Organization for Standardization as the effectiveness, efficiency, and satisfaction when using a system. These are the criteria from a human interaction perspective for software product standard. Also, the definition focuses on "specified users", "achieve specified goals" and "specified context to use" [5]. As stated by Jakob Nielsen (2012), usability is a qualitative attribute that tells us how easy something is to use. It is formed by five different attributes: learnability, efficiency, memorability, errors and satisfaction. These components form the overall experience of usability and usefulness [7].

HCI and usability have their origins back in 1980 when the prices of computers fell, so for the first time, it became possible for many employees to have their private computer (a.k.a pc). Then with the use of pcs in 1980 the users had no education or only a basic training on working with computer systems and software programs. However, software design practices continued to implicitly assume knowledgeable and competent users, who could understand technical vocabularies and system architectures, and they also have the ability to solve problems that arise from computer usage [8].

Due to this, usability became soon the key aim for the design of any interactive software that would not be used by the general public. It was then when popular phrases such as "user-friendly" entered everyday use. Both usability and user-friendliness had been first understood to be an asset of

interactive software. Unusable software programs could be made usable through re-design [8].

Web usability today is one critical term and a goal for every web design production. There are a lot of guidelines and sets of principles of good usability practices in general and for specific web usability. One well acknowledges set of rules began to craft during the founding of W3C in 1994. W3C provided the WACG (Web content accessibility guidelines) 1.0 in 1994 and 2.0 in 2008. These guidelines contain rules about permeability, operability, understandability and robust aspect of the content. These rules are highly technical and apply to coding parts of the webpages and the usability of the code itself. These rules are highly related to universal usability and good practices to improve accessibility [9]. According to Ben Shneiderman, a pioneer in the field of human-computer interaction, universal usability concerns "enabling all citizens to succeed using communication and information technology in their tasks." Designers who practice universal usability strive for designs that gracefully accommodate a diversity of user needs and circumstances [10].

## 2.2. Security and Privacy on OSNs

Privacy is a major concern for OSNs users. Apparently, this concern exists despite the extensive range of privacy control mechanisms that OSN users have at their disposal. Privacy in OSNs is a complicated issue that has been investigated many times by researchers of HCI and related areas focusing on the evaluation of controlling privacy settings on social networks and suggesting new prospects [12].

Privacy is an important issue in this context because, in most cases, the shared content (e.g., photos, location, and videos) refers to personal data, that without proper manage, may reveal users to unauthorised or malicious users. A user group, especially at risk of such privacy violations, are minors who typically share personal information publicly which might be more easily brought on or duped by malicious users [12]. Researchers on this path are critical to alert about vulnerabilities that this user group may be challenging, as well as to improve the usability of current privacy controls and to help in the improvement of new solutions that maximise the privacy of minors in OSNs [12].

Privacy could be defined as 'control over the flow of one's (personal) data, together with the transfer and exchange of that data'. Security is defined as 'the level that a user believes using a social networking website/application will not put him in any danger'. The major categories of privacy and trust in OSNs can be defined by the following measures:

- a) Security
- b) Control over the flow of data in a user's profile
- c) Notification

Security and trust concerns have a positive or negative effect on information sharing [13]. Also, other studies stated that as trust and privacy have an important role in real life, in face-to-face communication, and the improvement of new relationships, similar approaches seem to be used by users on OSNs [13].

The threats in social media increased with the growing numbers of users and usage. Users naively become exposed to various threats for their security and privacy. According to Fire et al (2014), in their article “Online Social Networks: Threats and Solutions” there are four main categories of threats in OSNs. These are:

1. Classic threats, the privacy and security threats
2. Modern threats, threats that exist in the field of OSNs and which use the OSNs structure and capabilities risking user’s security and privacy
3. Combination of threats, attackers combine different type of attacks, creating sophisticated attacks
4. Threats directed at minors users of social networks [15]

Privacy is a challenge for OSNs, is an issue that many researchers studied. Studying exciting models of privacy in social networks showed that often leak various types of private information. Several studies suggest that users have problems with a wide privacy control [14].

Studying and measuring privacy in general, is difficult, it’s even hard for the users themselves to quantify it [14]. A study conducted by Pew Research Center in the USA (2013) found out that most American users (86% percent) of OSNs take steps to cover their actions or identities online. About privacy controls, the results show that users believe that they are not to a level to protect their privacy. Another study by Pew focusing on parents and minors, concluded that most parents have concerns about their children privacy. At the same time teens seemed to have an understanding about different threats they can face online and they take steps to protect their privacy [16]. Similar results were found by an other Pew Research Center study that focused on teenagers. According to the results of that study, the majority (60%) of teenagers are taking steps to protect their privacy, keeping their profiles private and controlling the visibility only to selected friends. Similarly, 56% of them stated that they know, and they feel comfortable to change and manage the privacy settings at their Facebook accounts. Moreover, most teens claimed that they delete or block several users [17].

Today we have available different protection methods providing defences against spammers, threats, or different fake profiles. Research focusing on this problem by publishing studies with a goal to deal with various threats in OSNs and provide more improved suggestions in identity protection [15].

### **2.2.1 Sensitive Information**

As the use of OSNs becomes a daily habit for a lot of us, our personal information becomes easier to be exposed and maybe abused. These personal data are often collected by OSN operators and by third-party companies (commercial companies) this has recently been recognized as a new concern for the safety of OSNs users.

Sensitive content is information that may include age, gender, personal contact details and income. In some other cases, even more sensitive content (like sexual orientation) can be exposed.

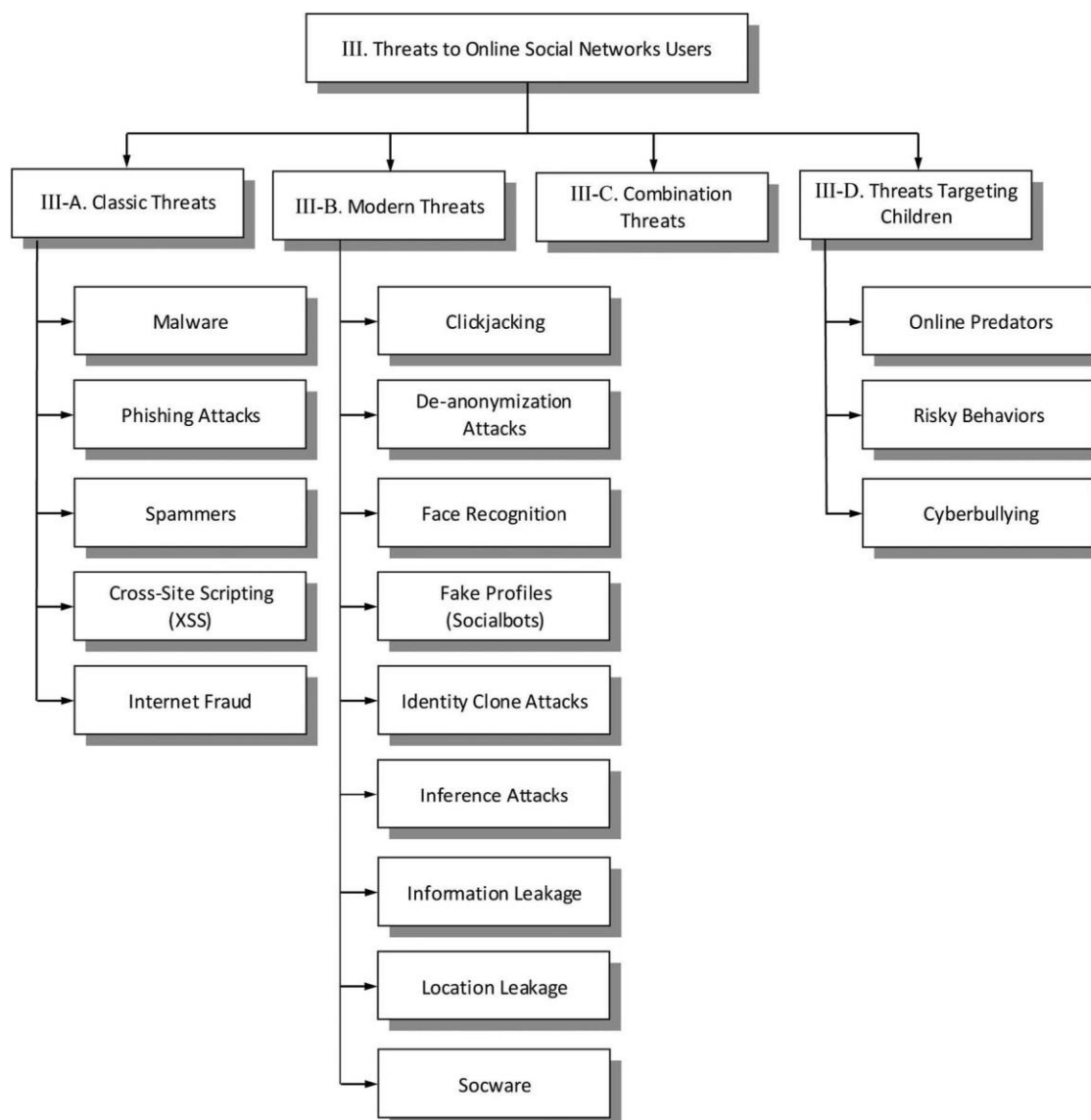


Figure 1. Threats to online social network users [15]

Users can protect their personal data in their online account from other users or suspicious third party installed applications controlling their privacy settings. For example, Facebook users can control the visibility of posts, pictures and personal details by adjusting their privacy settings as they like (choosing view setting such as to all Friends, Friends of Friends or Public for everyone) [15].

Some recommended solutions from threats in OSNs among others are the following: For better security and privacy it is suggested to the users to remove unnecessary personal information, data about themselves or their friends and family. It is also recommended changing the view of friend list to private. Furthermore deleting installed third-party applications is one extra action to take. A study with Facebook users showed that a thirty per cent of them had about forty applications installed on their accounts [12, 18].

One big study that was held as part of the “EU Kids Online II” project found different findings from the above studies. Around 25,000 children internet users (9-16 year old) from 25 countries participated in a survey. Results showed that in most countries younger children have their profiles public. Moreover, the users whose profiles are public appeared to provide more personal information than those users with private profiles. Around 50% of teen users of OSNs said that they have visible one or more of these three personal details on their online profile; the name of their school, their address or their phone number. Most common was the name of the school, but smaller percentages (15% of older and 12% of younger children have provided publicly their address or phone number too [19].



### **3. User Behavior and Experience when Faced with Security and Privacy Risks on OSN (study 1)**

This section includes, an extensive literature review on user behavior and experience when faced with security and privacy risks on OSN. Although there are several studies on behavior of users, as well as on the identification and recording of threats, risks and attacks on OSNs [20, 21, 22, 23, 24, 25, 26], there is a lack of studies regarding the users’ behavior when facing privacy and security risks. This review intends to fill this gap by a comprehensive study and analysis of users’ behavior in social networks, highlighting the risks to privacy and vulnerabilities of user safety on OSN.

The review is based on the collection and critical analysis of more than 70 research articles published the last years in scientific journals and proceedings of international conferences. Several aspects related to the user behavior, security and privacy risks, and user behavior when facing security risks were studied.

#### **3.1. User behavior on OSN**

McGrath (2017) [27] by analyzing the trends in OSN and exploring the main reasons of their use, concluded that: users among 16-24 year-olds use social media to fill up spare time, the users among 25-34 year-olds use social media to stay in touch with their friends, while the users among 34-44 year-olds use the social media to stay up-to-date with news and current affairs. Many studies have tried to identify the factors that affect users’ participation in OSN [28, 29, 30]. The Internet self-efficacy, need to belong, and collective self-esteem have positive effects on users attitudes toward OSN. Specifically, user attitude toward OSN mediates the relationship between willingness to join OSN and: (i) Internet self-efficacy and (ii) need to belong, and the mediation is only partial between willingness to join and collective self-esteem [28].

Despite widespread warnings of the dangers of poor online safety practices, a surprisingly high percentage of users are still very naive about safety [25, 31]. However, as the reasons for the use of OSN differ, the privacy concerns, trustiness and users’ behavior, towards them also varies. There are users that take into account the OSN’ risks and adhere to the necessary security settings, as well as there are ignorant users directly exposed. Yao et al. (2007) [21] have revealed that beliefs in privacy rights and a psychological need for privacy were the main influences on online privacy concerns. Fogel & Nehmad (2008) [32], exploring risk taking, trust, and privacy concerns with regard to OSN, among 205 college students (17-32 years old), found that individuals with profiles on social networking websites have greater risk taking attitudes than those who do not, while greater risk taking attitudes exist among men than women.

#### **3.2. Risks, threats, attacks and privacy leakage on OSN**

The chaotic nature of the Internet, coupled with the lack of adequate and rigorous legislation and the lack of effective information and online education, favor the existence and spread of security risks. There is a wide variety of risks and threats on the web and OSN that are evolving over time. According to [23] the OSN threats can be divided into 4 main categories: i) classic threats, ii) modern

threats, iii) combination threats, and iv) threats targeting to children. Regarding to children, pedophilia and cyber-bullying are the greatest scourges on the Internet [20, 33, 34]. A study by Hugi (2011) [35] indicated that: i) adults seem to be more concerned about potential privacy threats than younger users, ii) policy makers should be alarmed by a large part of users who underestimate risks of their information privacy on OSN, and iii) in the case of using OSN and its services, traditional one-dimensional privacy approaches fall short. Although OSN permit users to control what they share and with whom, access control policies are notoriously difficult to configure correctly. Madejski et al. (2011) [36] have investigated whether OSN users’ privacy settings match their sharing intentions via an empirical evaluation, in which privacy attitudes and intentions have been measured and compared against the privacy settings on Facebook. Their results have indicated that every one of the 65 participants confirmed that at least one of the identified violations was in fact a sharing violation and a majority of users cannot or will not fix such errors. Furthermore, they have concluded that the current approach to privacy settings is fundamentally flawed and cannot be fixed. Over time and the social networks evolution, privacy control mechanisms have been improved so that users can determine who can see their personal information. However, sensitive user information could leak even when privacy rules are configured correctly [37].

### **3.3. Users behavior when faced privacy risks on OSN**

The behavior, when users face privacy risks on OSN, varies and is difficult to be clarified and predicted. Even if many actions have been taken by OSN to provide security and privacy to their users, justifiably, it cannot be claimed that the current level is adequate. On the other side, users must understand that they cannot arbitrarily share content with other users and services. Users’ content can be used in many ways, many of which can be proved to be malicious. User awareness through proper notifications might help in this direction, but clearly more media coverage and education can greatly help in this aspect [38].

The work of Angulo & Ortlieb (2015) [39] is one of the very few which aims to unveil and understand common online privacy panic situations. The authors presented an exploratory study on common experiences of online privacy-related panic and on users’ reactions to frequently occurring privacy incidents. By using the metaphor of a privacy panic button, they have investigated users’ expectations and mental models of suitable help mechanisms that could lead these users towards a solution, calming their distress, and preventing similar episodes from happening in the future. Through user semi-structured interviews (n = 16) and a survey (n = 549), they have identified 18 scenarios of privacy panic situations. The results have shown that victims’ topmost worries included possible harm to their finances or fear of embarrassment, as well as third-parties knowing things that might not be of their business. Among the most memorable self-reported panic stories were cases of account hijacking and ‘leakage’ of personal data, while incidents involving regrets when sharing content online were found to be experienced most frequently. However, scenarios related to the loss of online data, the loss of a mobile device, or falling pray of identity theft also were at the top of users’ concerns. Their findings also indicate that, in the case a service provider were to offer a hypothetical privacy panic button; users would expect that the help provided is immediate, uncomplicated, actionable, and in-place.

## 4. Meta-review on Cyberbullying (study 2)

### 4.1. What is Cyberbullying

Perhaps one of the most widely accepted definitions of Cyberbullying comes from [40] defining cyberbullying as “an aggressive intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself” (p. 376). Generally speaking, cyberbullying can be seen as any form of abusive behavior in cyberspace. A typology of cyberbullying behavior has been proposed by Nocentini et al. [41] and includes four type of activity: written-verbal behavior (phone calls, text messages, e-mails, instant messaging, chats, blogs, social networking communities, websites), visual behavior (posting, sending or sharing compromising pictures and videos through mobile phone or internet), exclusion (purposefully excluding someone from an online group) and impersonation (stealing and revealing personal information, using another person’s name and account). Research has demonstrated a number of negative effects of cyberbullying victimization including lower self-esteem, retaliating, and being scared, frustrated, angry and depressed [42]. When the victim fails to cope with the emotional tension of the abuse, the consequences of cyberbullying become even more serious leading to suicidal thoughts and behavior [43, 44].

### 4.2. Methodology

In order to understand scholarly activity on cyberbullying, we first compiled the corpus of research on cyberbullying using keyword search in scientific databases across disciplines -- from social science and humanities to computer science. A taxonomy of the cyberbullying key-terms has been presented by [45] which includes the terms cyber-bullying, cybergrooming, cyber-stalking, electronic bullying, sms bullying, mobile bullying, online bullying, digital bullying, e-bullying, and Internet bullying. This taxonomy formed our basic keyword search, which was expanded to include more terms, considering the keywords and ideas presented in the manuscripts themselves, such as predator, victim, bystander, harassment, trolling, aggressive behavior, distressed behavior, hate speech, content monitoring, doxing, and cybermobbing. A summary of our findings is provided below.

### 4.3. Results

**The Profiles of the Main Actor:** There are three main actors in the cyberbullying menace: the predator, the victim, and the bystander.

**Cyberbully:** In an overview of research on the types of cyberbullies (also cyberbullying perpetrators or predators), [46] identified five main categories, taking into account the psychological attributes (both personal and social) that underpin their behavior: the sociable cyberbully; the lonely cyberbully; the narcissistic cyberbully; the sadistic cyberbully; and the morally-driven cyberbully.

**Cybervictim:** Much of the previous research has attempted to identify risk factors for bullying and cyberbullying (typically examined together) focusing on demographic and behavioural measures. A number of psychological variables emerged in different studies describing the cybervictim. Sourander et al. [48].

**Bystander:** The third actor in cyberbullying is the (negative) bystander who observes bullying without taking action. A comprehensive study of this actor comes from [49] who found that three factors increased the likelihood of negative bystander behavior: (i) the cyberspace, meaning that negative bystander behavior occurs more often in the cyberspace than offline, (ii) the private nature of the act, meaning that bystander behavior might occur more frequently in private forms of violence, and (iii) the experience of being a cyberbullying predator seems to be important predictor of negative bystander behavior.

**A Typology of Cyberbullying Actors:** A typology of cyberbullying actors in terms of their personal characteristics has yet to be presented in the cyberbullying literature. Instead, findings are sparse and inconsistent, calling for more work in this area.

**Gender:** Inconsistent findings have been reported regarding gender. Although research on traditional bullying shows that bullying is more common among boys (e.g., [50]), for cyberbullying, findings are mixed. A study showed that girls were more likely, than were boys, to report cyberbullying as predators, especially in combination with school bullying, but they were also more likely to be victims of both types of bullying (on school property and cyber) [44].

**Age:** While traditional bullying seems to peak during middle school, cyberbullying peaks somewhat later [57]. In fact, with age, there seems to be a gradual shift away from traditional forms of bullying such as spreading rumours, to cyberbullying.

**Sexual Orientation:** There seems to be a consistent finding that non-heterosexual individual are targets of traditional bullying and cyberbullying. For example, [44] reported that non-heterosexual youths were more likely to be victims of cyberbullying, compared to heterosexual (10.5% vs 6.0%). A previous study reported similar findings, showings that lesbian, gay, bisexual, and transsexual individuals were twice as likely to experience cyberstalking or e-mail harassment from a stranger, compared to heterosexual individuals.

**Other Personal Characteristics:** A few other profile patterns of cyberbullying actors have been reported in the literature as follows:

1. Computer use. Students who were victims, bullies, and bully–victims were more likely than students who were not involved in cyberbullying to use the computer for more hours a day and to give their password to friends [56]. Also, intensive use of the Internet emerged as a risk factor for child cyber-harassment [60]. Furthermore, the location of the computer at home was found to be a predictive factor of cyber victimization. Children who use the computer in private places at their home (e.g., bedroom) were at higher risk to be victimized than children who used computers in a public space in their home [61].
2. School performance. According to [44], youth who reported lower school performance and lower school attachment were also more likely to be victimized with cyberbullying; in particular, students who received mostly Ds and Fs were twice as likely to be victims of cyberbullying compared to students who received mostly As (11.3% vs 5.2%).

3. Bullied person, bullying others. There is a lack of research on the bully-victim group (persons being bullied and also bullying others) whilst a potential causal link is alarming and warrants further investigation (Does bullied person become a bully?). For example, in their survey research, [47] found that previous offline bullying and victim experiences were associated with more cyberbullying. Similarly, Mishna et al. [56] argued that the cyber offers easy space for “revenge” or “payback” with high prevalence of bully-victim behavior (26%) in a sample of 2186 participants [56].

**The Problematic Nature of the Label “cyberbullying”:** Defining, measuring, or detecting specific cyberbullying behavior is not a trivial task. Existing definitions of cyberbullying, as well as the one adhered in this review by [40], often incorporate the criteria of traditional bullying such as repetition over time and imbalance of power (a victim who cannot easily defend him/herself). However, due to the unique nature of cyber-based communication, it is difficult to identify such criteria in the cyber abuse [62]. As a result, there is uncertainty regarding the operational definition of cyberbullying and how to effectively measure it [62].

**The Power Dimension:** Although a central aspect of most operational definitions of traditional bullying, “power” is difficult to determine in the cyber context [62]. Is “power” the ability to remain anonymous in the cyberspace [40]? Is it the ability to demonstrate superior technological knowledge [64]? Is it the immediacy of content dissemination and capacity to humiliate on a grand scale [65]? Or is “power” the perceived popularity of the predator causing more psychological distress? The later was investigated by [66] who found that, compared to being harassed by an unpopular cyberbully, being harassed by a popular cyberbully was more distressing and elicited more negative mood and helplessness. Understanding what “power” in cyberspace entails will significantly inform the operational definition of cyberbullying.

**The Dimension of Severity - Duration and Level of Insult:** Cyberbullying can occur anytime and anywhere and is believed to be more damaging than traditional face-to-face bullying because of the fluidity and frequency of the bullying behavior using technology. In fact, several authors [65, 67] hypothesised that because bullying acts performed online are visible for a long(er) period of time and to a large audience (who may also join the bully), their negative effects can be more severe and longer lasting, compared to victims of repeated (offline) bullying acts. Yet, there is lack of empirical research tackling cyberbullying as a sequence of actions that involve repetition of harming content and levels of severity. Potha and Maragoudakis [68] seem to be the first to have considered the duration and level of insult in cyberbullying; using a dynamic time warping algorithm, they were able to provide an immediate indicator for the severity of cyberbullying within a given dialogue. Yet, more research is needed for understanding (and detecting) the level of insult and duration of the cyber abuse.

**The Anonymity Dimension:** The anonymity in cyberbullying adds a totally new dimension to the nature of traditional bullying. The devices that are used (such as mobile phones and computers) make it easier for a perpetrator to act anonymously (e.g., by using a nickname) and without directly facing the victim [69]. Moreover, cyberbullies have less chance of getting caught or punished as they can perpetrate without adult supervision [40]. What makes the anonymity dimension more apparent

in cyberbullying, is the evidence that many cyberbullies do not choose in- person bullying if the cyber route is denied. As [70] discussed, cyberbullies might not bully in person because they feel powerless socially or because they are invested in school and academics, but are willing to bully online because they believe that cyberbullying is without risk since adults are not present.

While there is an unceasing flow of media stories reporting cases of cyberbullying, particularly within online social media, research efforts in the academic community are scattered over different topics and across the humanities and computer science. The majority of academic contributions focus on understanding the phenomenon, risk factors and threats with the prospect of suggesting possible protection strategies. Detecting cyberbullying when it occurs and identifying predators and their victims in real computer- mediated communication remains an open issue to be solved, before intervention and prevention methods can be addressed. Recognizing blocks of cyberbullying activity and understanding dimensions such as duration, severity, power, and anonymity can shed valuable insight into how cyberbullying is fed and evolves. There is an immediate need for true multidisciplinary work between social and computer sciences, in order for current challenges to be effectively addressed and significant progress to be made, and we are confident that this review will serve as a multidisciplinary agenda to guide future research in this area. Africa is an under represented continent in such studies. Studies that document cyberbullying in Africa, ways of combatting it in such communities and mechanisms for encouraging training and awareness for young communities on online behavior and protection [71].

## 5. E-safety in Web 2.0 Learning Environments (study 3)

This study explored the research development pertaining to safety and security in Web 2.0 learning environments, as well as a review of web-based tools and applications that attempt to address security and privacy issues in Online Social Networks. This work [81] was published in HCI International 2017 and argues that Web 2.0 learning environments entail threats and challenges in the safety of both students and instructors, and further research needs to take place for handling and protecting the privacy of all involved stakeholders.

The advancement of Web 2.0 tools offers a rewarding source of knowledge sharing, interaction and socialization. Web 2.0 is considered “a catch-all term to describe a variety of developments on the web and a perceived shift in the way the web is used. This has been characterised as the evolution of web use from passive consumption of content to more active participation, creation and sharing – to what is sometimes called the ‘read/write’ web” [1, p. 9]. This term encompasses technologies that emphasize social networking, collaboration and media sharing such as Facebook, Twitter, Snapchat and MySpace. Amongst the benefits reported in the use of these tools include the development of 21st century skills such as creativity, innovation, team building, critical thinking, information sharing, higher academic achievement and improvement of ICT skills and competences [2–5]. Despite the popularity of Web 2.0 technologies, they still receive concerns by students and teachers with regard to their ability to support learning in a secure environment. Being present in online social networking sites presents particular risks such as exposure to cyberbullying, child abuse, inappropriate material and contact with dangerous strangers. Social Web can facilitate abuse of children by adults - being in place to assume fake identities online, a possible “danger” can intrude a child’s private zone leading to violence or even sex crimes [6]. The risks and threats that minors encounter on the internet can be classified under the following five categories [7–9]: (a) content risks: instances or events in which children are exposed to illegal harmful or age inappropriate content and harmful advice; (b) contact risks: instances or events in which children have direct interaction with other children or adults. Frequent threats under this category are cyber-grooming (i.e. adults trying to develop relationships of trust with children with the aim of having sexual intercourse with them) and cyberbullying; (c) Children targeted as consumers: instances or events in which children face the risk of being treated as consumers of products and/or services designed only for adults; (d) Economic risks: instances or events in which children spent money in gambling and other online games; (e) Online privacy risks: instances or events in which children share personal data with inappropriate audience.

A fundamental dilemma that practitioners need to address when considering the use of Web 2.0 tools for minors relates to e-safety and privacy. The question is timely in light of current upsurge of Web 2.0 technologies in educational environments, where researchers and/or instructors attempt to integrate such tools in the learning environment without violating students’ safety and personal rights. The question has attracted researchers and practitioners attention as it is evident from

research papers and conferences (cf. Special issue of *Computers & Security Journal* on trust in cyber, physical and social computing). Some studies have been guided by the wish to understand students and teachers’ concerns in incorporating Web 2.0 technologies in the classroom (cf., for example, [10]) and some by the wish to identify methods for handling e-safety in a cost-effective way (cf., for example, [11]).

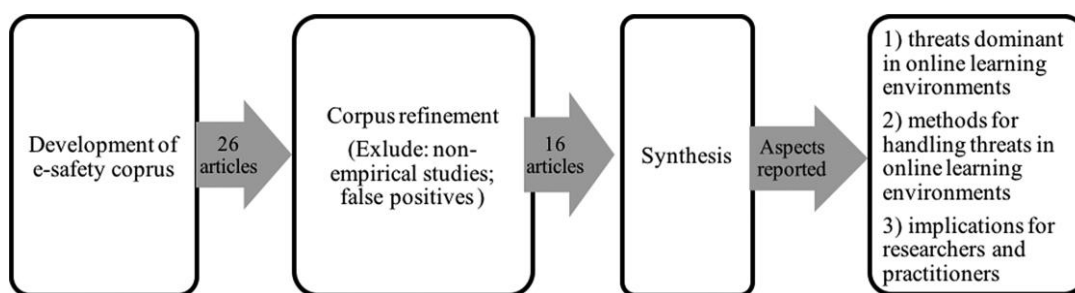
This paper provides the state-of-the-art regarding e-safety in the use of online collaborative environments delineating tools and threats dominant in Web 2.0 learning environments; methods and tools for handling these threats, as well as implications for researchers and practitioners.

### 5.1. Methodology

With an eye to synthesizing the findings of research regarding e-safety in Web 2.0 learning environments, we followed a three-step approach as demonstrated in Fig. 5. Our approach included: (a) compilation of the e-safety corpus which included research manuscripts related to e-safety from manual search in scientific databases; (b) refinement of the e-safety corpus and (c) synthesis of the research papers.

The methodology of this review was informed by previous studies such as Parmaxi, Zaphiris, Papadima-Sophocleous and Ioannou [4] who reviewed recent research development in Computer-Assisted Language Learning and Parmaxi and Zaphiris [5] who reviewed the use of Web 2.0 tools in Computer-Assisted Language Learning.

In order to capture scholarly activity in e-safety in Web 2.0 learning environments, we started by selecting appropriate resources which compiled the e-safety corpus.



**Figure 2. Flow diagram of the methodology adopted for exploring scholarly activity in e-safety in online collaborative environments**

Appropriate articles for inclusion were selected via manual keyword search in manuscripts’ title, abstract and given keywords. The keywords for searching were “security”, “safety”, “e-safety”, “social media”, “education”, “learning”, “threat”, “Web 2.0” in the following databases: ERIC, Education Research Complete, Academic Search Complete, Computers & Applied Sciences Complete, Springer Link, Research Starters, Psychology and Behavioral Sciences Collection, Food Science Source, Taylor & Francis Group. The keyword search returned 26 manuscripts which comprised the



preliminary e-safety corpus of this review.

The corpus was then refined in order to meet the objectives of this review. Each manuscript was scanned in order to elucidate the aim of each study. This stage facilitated the optimization of the e-safety corpus, as we excluded articles that were incorrectly selected in the search process (false positives) as well as articles reporting on non-empirical studies. The final e-safety corpus included 16 manuscripts.

Each paper in the e-safety corpus was then examined in depth, extracting information related to the following pre-defined aspects: (1) threats dominant in online learning environments; (2) methods for handling threats in online learning environments and; (3) environments; (2) methods for handling threats implications for researchers and practitioners.

## 5.2. Findings

Recent debates about students’ activities with Web 2.0 technologies strive between their perceived benefits and their potential threats. The social web is seen to have the capacity to foster formal and informal learning, yet students, teachers and parents demonstrate increased concern about the online risks and threats, often related to child sex abusers, and bullying, as well as concerns related to the safe presence of a school community in Online Social Networks (OSNs). Concerns about online safety fit within a broader agenda related to students’ e-safety, recognizing the need to develop the skills and competences needed for taking advantage of the benefits that ICTs can provide. Figure 6 provides an overview of e-safety in Web 2.0 learning environments as derived from the e-safety corpus. The classification of the e-safety corpus demonstrated four categories that can be summarized as follows: (a) students’ and teachers’ attitudes and experiences towards e-safety in OSN, (b) e-safety actions, practices and policies in OSNs, (c) evaluation of schools’ e-safety regulations in OSNs and (d) internet safety education.

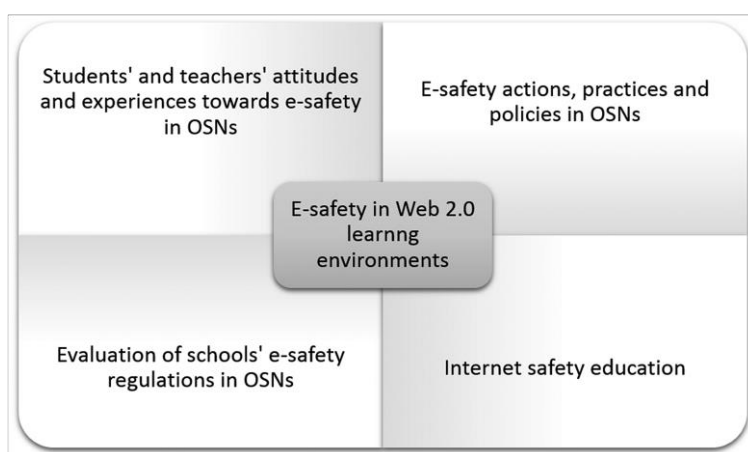


Figure 3. Overview of e-safety in Web 2.0 learning environments as derived from the e-safety corpus

### 5.2.1 Parents' and Teachers' Attitudes and Experiences Towards E-safety in OSNs

This category entails manuscripts that deal with students' and teachers' attitudes and experiences towards e-safety in the use of OSN. For example, Sharples, Graber, Harrison, and Logan [10] report results of a study that explored children's, teachers', parents', managers' and technical staff's understanding of Web 2.0 activities and concerns. Findings demonstrated that a high percentage of the children surveyed (74%) have used social networking sites (SNS), whilst a substantial minority interacted regularly online with people they have not met face-to-face. Although teachers demonstrated the desire to take advantage of the benefits of Web 2.0 for creative and social learning, / they reported being limited by a need to show a duty of care that prevents worst-case risk to children, to restrict access to SN sites. The respondents also reported concerns about Internet bullying and exam cheating. Finally, a Policy Delphi process voiced the need for schools to allow access to Web 2.0 sites, but educate children in responsible and creative learning.

### 5.2.2. E-safety Actions, Practices and Policies in OSNs

In this category, researchers engage in online safety actions, practices and policies. For example, Searson, Hancock, Soheil, and Shepherd [12] describe the need for developing informed policies and practices that would involve a wide range of sectors of the society. Such practices would inform technology integration in educational settings addressing the following factors: national and local policies, bandwidth and technology infrastructure, educational contexts, cyber-safety and cyberwellness practices and privacy accountability. Two organizations offer examples and set guidelines for digital citizen-ship in educational settings, that is ISTE (<https://www.iste.org/explore/ArticleDetail?articleid=101>) and iKeepSafe (<http://ikeepsafe.org/>). On the same line, Waters [11] highlight the multifarious security challenges that school districts encounter, using as a stepping stone the example of a high school's page that has been hijacked by a former student. The manuscript concludes by suggesting two web browser add ons Firesheep and BlackSheep for users on unsecured WiFi networks to identify the social networking sessions of others on that Network. Similarly, the Parent Teacher Association demonstrates its action in educating children and parents about Internet Safety [13]. On the same line, Ramnath [14] discusses how school administrators can protect students' safety while integrating technological advancements in teaching and learning. The study engages in topics such as cyberbullying and cyberstalking, the use of social networking sites for collaboration and the use of Mobile Device Management for the safety of mobile devices within and outside the school network. Similarly, Campbell-Wright [15] examine e-safety in e-learning, the benefits and dangers of online interaction and guide- lines for preparing organizations to handle e-safety. Similarly, Wespieser [16], upon a survey distributed in 14,309 young people in London, demonstrated the high percentage of internet usage and social network sites, as well as issues of bullying and exposure to inappropriate material. The British Educational Communications and Technology Agency (BECTA) investigated the use and impact of Web 2.0 technologies in and out of school [10]. Findings demonstrated that at Key Stages 3 and 4, students harness extensively Web 2.0 outside of school, and for social purposes. The major challenge for schools in considering the usage of Web 2.0 technologies is how to support children to engage productively and creatively in social learning while protecting them from potential risk. Most learners demonstrated awareness of internet dangers, though many performed poorly in e-safety (e.g. in practice around password security). Whilst parents are generally positive in the use of technology for learning, yet concerns about e-safety exist. The paper concludes with indicating

schools’ responsibility in raising children’s awareness on safe engagement with Web 2.0 and the internet in general. Triggered by educators’ fear to adopt social networking in their teaching, Blazer [17] sets off to review the opportunities and challenges associated with education-based social networking, providing recommendations for schools when they are establishing social networking policies. Despite the risks that schools encounter when exposing students in social networking sites, their use in the classroom can promote academic learning and increase student engagement. Recommendations provided include the formulation of strong policies that address harmful online interactions and provide educators and students with guidance in the use of OSNs. Moreover, non-commercial sites are available and can monitor access to social media. Crook and Harrison [1] also capture the importance to distinguish the current fears of society from evidence of actual risk to children. They demonstrate that the majority of learners in Key stages 3 and 4 are aware of online safety, yet, they demonstrate the need for schools and teachers to have a key role in students’ e-safety. Experts participating in the study favored the empower and manage approach, i.e. schools to allow free students’ access to public Web 2.0, but children need to be educated on how to use Web 2.0 activities for responsible and creative learning. Children’s web activity needs to be monitored for action to be taken against threatening or unsafe online behavior. Similarly, Sutton [18] provides 7 things to know right about campus security: (a) address sexual assaults on campus; (b) develop a social-media network for resources and campus security officials; (c) increase awareness of law enforcement in the higher ed community; (d) provide Web training on current topics; (e) develop crime prevention programs that are customizable; (f) put into place adequate social-media policing policies; (g) understand what the new Violence Against Women Act (VAWA) requirements mean for your campus.

### 5.2.3. Evaluation of Schools’ E-safety Regulations in OSNs

Being in place to understand and evaluate schools’ e-safety regulations is an issue that attracts high interest from researchers. On this line, Lorenz, Kikkas, and Laanpere [19] analyzed the types and sources of safety incidents, the solutions offered, the students’ reactions from these incidents and the solutions suggested by students. Findings demonstrated that many students do not understand what e-safety is, assuming that they are not involved in any way in an e-safety episode, even if they have suffered from an online attack. The awareness training about “stop-block-tell” does not work as it is radically different from the way students think and act in real life situations. Blocking unwanted material is the least successful solution for the students, even if current typical awareness training is focusing on it. As findings demonstrated, students seem to be passive reactors to any malicious behavior, thus training focusing on stop-block-tell” or “don’t click everywhere” seems unsuccessful. The solution provided by authors “is to include more technical and other practical aspects in the awareness training and distribute step-by-step, common-language how-to-s like how to set one’s privacy settings, how to report a page, picture, video or how to behave when someone is being bullied, or what to do when one becomes a victim of fraud or slander. The awareness in these areas is also needed for the adults who are setting the standard how their students or children behave and deal with the problems in the future” [19, p. 336]. Ultimately, it is of major importance for schools to develop policies, strategies and solutions that address the core issues of children.

Following a similar path, Lorenz, Kikkas, and Laanpere [20] explored 201 e-safety related stories

presented by students (age 12–16), parents, teachers, school IT managers and police. Through the stories, typical behavioral patterns were mapped, beliefs, regulations and limitations regarding the use of social networks in schools in Estonia. The results demonstrated that few schools hold an explicit policy for e-safety issues. Yet, even these few school-level policy documents fall behind in tackling the topics which were most frequently mentioned in students’ stories. Safety incidents related to cyberbullying or exposure to illegal material remain unsolved or even undetected. Schools delegate any safety incidents to parents who in turn look to schools for assistance. As a principle, e-safety policies should focus on topics with which all stakeholder groups agree being important: gaming, fraud, password, harassment, pornography and meeting strangers. Emphasis should be placed in assessing e-safety risks and how they can influence online learning activities. Similarly, Cranmer [21] reports on excluded young people’s experiences of e-safety, demonstrating that the strategies they employ to manage their online safety are primitive and insufficient, thus pointing the need for developing further their online strategies and ultimately their digital literacy.

#### **5.2.4. Internet Safety Education**

Internet safety education is a topic that attracts researchers’ interest, as advancement of technological systems calls for schools to teach children to protect themselves on the web. Whilst internet safety was introduced with some “special occasion” events or a dedicated “Internet Safety Day”, yet these actions seem to serve no purpose and have no real learning impact [22]. On this line, Naidoo, Kritzinger, and Look [23] present a cyber –safety awareness framework that introduces cyber safety awareness education to primary school children in the South African community. The cyber safety awareness framework offers multifarious benefits for bridging the lack of cyber safety awareness both in schools and in communities. The framework proposes that schools are grouped into clusters, with a cluster coordinator as its head. Cyber safety awareness information is expected to be disseminated through workshops attended by teacher representatives of these school clusters, and distributed back to parents, children, other teachers and ultimately to their communities. On the same line, Orech [22] elaborates on the Digital Citizenship Project that aimed at integrating Internet Safety in the educational curriculum. Through the programme, students learned about cyberbullying and prevention as well as strategies for protecting themselves in case of a cyber-insult. The project had successfully employed social media for engaging middle school teachers and students to discuss about netiquette, digital citizenship, cyber crime prevention and managing digital footprint. Ultimately, sophomore students and teachers become cybermentors engaging in conversations about cyberbullying prevention and protection. Following a somewhat similar path, Moreno, Egan, Bare, Young, and Cox [24] consider internet safety education of vital importance for youth in US, thus they surveyed at what age should such education begin and what group is held responsible for teaching it. Having distributed their survey to 356 teachers, clinicians, parents and adolescents they demonstrated that the optimal age for internet safety education is 7.2 years ( $SD = 2.5$ ), whilst parents were identified as the stakeholder with the primary responsibility in teaching this topic. Clinician’s role was also recognised as vital in providing resources, guidance and support.

#### **5.2.5. Implications for Researchers and Practitioners**

As the usage of Web 2.0 technologies advances, the more instructors and students engage with these technologies in and out of school. Internet usage has changed the way literacy is perceived

and taught, raising the crucial need not only for information literacy, but also for digital literacy and specifically e-safety education. In this endeavour, the question of how parents and educators can accommodate children’s behaviour on the net still needs to be further investigated. Prohibiting the use of OSNs, blocking the use of unwanted material or even blocking the use of internet in the school environment is the least successful solution. As noted by Lorenz, Kikkas, and Laanpere, [19] there is a need for more technical training; as well as more automated solution that would set one’s privacy settings, instructing on how to report a page, picture, video or how to react when someone is being bullied. Taking into consideration the high percentage of internet usage and social network sites, there is a strong need in engaging children productively, responsibly and creatively in social learning while protecting them from potential risks. Whilst children are aware of internet dangers but perform poorly in applying e-safety, rises schools’ responsibility in raising children’s awareness by providing cyber-safety and cyberwellness practices. Thus, providing online and on-site training for both teachers and parents for confronting the challenges of the new digital era with practical guidelines on e-safety and privacy is vital. With this in mind the next section provides a review of existing web-based tools and mobile applications that attempt to address security and privacy issues in Online Social Networks.

### 5.3. Conclusions

As the Internet and Communication Technologies expand rapidly in many everyday activities, concerns are raised with regard to the safety of a vulnerable group such as children on the web. As noted by O’Brien, Budish, Faris, Gasser, and Lin [42], cyber- security incidents are reported each year sitting at the top of government policy and boardroom agendas. Our findings demonstrate that recent research activity related to safety in Web 2.0 technologies pertains to: (a) students’ and teachers’ attitudes and experiences towards e’-safety in OSNs, (b) e-safety actions, practices and policies in OSNs, (c) evaluation of schools’ e-safety regulations in OSNs and (d) internet safety education.

The incorporation of OSNs in the classrooms confronts educators with new opportunities and challenges as there is an increasing need for educating children on productive, creative, safe and responsible engagement in the use of OSNs. More work is needed in the provision of online and on-site training of both teachers and parents for confronting the challenges of the new digital era and for putting together a comprehensive e-safety framework in order to include practical guidelines on e-safety and privacy. Blocking the use of OSNs in the school environment provides only a shallow solution to the problem; there is a need for providing students the skills for managing potential risks on the web by properly setting their privacy settings, reporting inappropriate material and reacting to cyber threats.

Moreover, there is an urgent need for designing effective measures against internet risks and threats, as well as for understanding minors’ activities online. Most of the existing parental/educational control software rely on monitoring and parent/educator review to detect any abnormal activity. Some of them search for keywords to create alerts, while some others block the usual list of websites. Cyber-bullying, cybergrooming, and exchange of sensitive content is not intelligently detected by existing web-based tools and this has a negative social effect on the

children i.e. they are monitored to an excessive degree and this will probably lead them to find alternative ways to go online. Existing Internet filtering techniques for protecting minors online need to be redesigned and reapplied in a smarter way, by incorporating more sophisticated techniques such as data analytics, advanced content analysis and data mining techniques that could allow for OSN fake account identification and sexual content detection.

#### 5.4. Subsection References

1. Crook, C., Harrison, C.: Web 2.0 technologies for learning at key stages 3 and 4: summary report (2008). [http://dera.ioe.ac.uk/1480/1/becta\\_2008\\_web2\\_summary.pdf](http://dera.ioe.ac.uk/1480/1/becta_2008_web2_summary.pdf)
2. Wright E.R., Lawson A.H.: Computer-mediated communication and student learning in large introductory sociology courses. In: Paper presented at the Annual Meeting of the American Sociological Association, Hilton San Francisco & Renaissance Parc 55 Hotel, San Francisco, CA (2004). [http://citation.allacademic.com/meta/p\\_mla\\_apa\\_research\\_citation/1/0/8/9/6/pages108968/p108968-1.php](http://citation.allacademic.com/meta/p_mla_apa_research_citation/1/0/8/9/6/pages108968/p108968-1.php)
3. Green H., Hannon C.: TheirSpace: Education for a Digital Generation. Demos, London (2007). <http://dera.ioe.ac.uk/23215/1/Their%20space%20-%20web.pdf>
4. Parmaxi, A., Zaphiris, P., Papadima-Sophocleous, S., Ioannou, A.: Mapping the landscape of computer-assisted language learning: an inventory of research. *Interact. Technol. Smart Educ.* 10(4), 252–269 (2013). doi:10.1108/ITSE-02-2013-0004
5. Parmaxi, A., Zaphiris, P.: Web 2.0 in computer-assisted language learning: a research synthesis and implications for instructional design and educational practice. *Interact. Learn. Environ.*, 1–13 (2016). doi:10.1080/10494820.2016.1172243
6. Wolak, J., Finkelhor, D., Mitchell, K.J., Ybarra, M.L.: Online ‘predators’ and their victims: myths, realities and implications for prevention and treatment. *Am. Psychol.* 63, 111–128 (2008)
7. Dooley, J., Cross, D., Hearn, L., Treyvaud, R.: Review of existing Australian and international cyber-safety research. Child Health Promotion Research Centre, Edith Cowan University, Perth (2009)
8. OECD: The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them. OECD Digital Economy Papers, No. 179. OECD Publishing, Paris (2011). <http://dx.doi.org/10.1787/5kgcjf71p128-en>
9. Tsirtsis, A., Tsapatsoulis, N., Stamatelatos, M., Papadamou, K., Sirivianos, M.: Cyber security risks for minors: a taxonomy and a software architecture. In: 2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP), pp. 93–99. IEEE, November 2016
10. Sharples, M., Graber, R., Harrison, C., Logan, K.: E-safety and web 2.0 for children aged 11–16. *J. Comput. Assist. Learn.* 25(1), 70–84 (2009)
11. Waters, J.K.: Social networking: keeping it clean. *THE J.* 38(1), 52 (2011)
12. Searson, M., Hancock, M., Soheil, N., Shepherd, G.: Digital citizenship within global contexts. *Educ. Inf. Technol.* 20(4), 729–741 (2015)
13. A Safer Digital World. *Our Child.* 39(5), 5 (2014). ISSN 10833080
14. Ramnath, S.: How schools can keep students safe, and on Facebook. *eSchool News* 18(4), 16 (2015)
15. Campbell-Wright, K.: E-safety. NIACE (2013)
16. Wespieser, K.: Young People and E-safety: The Results of the 2015 London Grid for Learning

- E-safety Survey. National Foundation for Educational Research (2015)
17. Blazer, C.: Social Networking in Schools: Benefits and Risks; Review of the Research; Policy Considerations; and Current Practices. Information Capsule, vol. 1109. Research Services, Miami-Dade County Public Schools (2012)
  18. Sutton, H.: Review the top 7 things to know right now about campus security. Campus Secur. Rep. 12(4), 1–5 (2015)
  19. Lorenz, B., Kikkas, K., Laanpere, M.: Comparing children’s E-safety strategies with guidelines offered by adults. Electron. J. e-Learn. 10(3), 326–338 (2012)
  20. Lorenz, B., Kikkas, K., Laanpere, M.: Social networks, e-Learning and Internet safety: analysing the stories of students. In: Proceedings of the 10th European Conference on e-Learning ECEL-2011: 10th European Conference on e-Learning ECEL-2011, Brighton, UK, pp. 10–11, November 2011
  21. Cranmer, S.: Listening to excluded young people’s experiences of e-safety and risk. Learn. Media Technol. 38(1), 72–85 (2013)
  22. Orech, J.: How it’s done: incorporating digital citizenship into your everyday curriculum. Tech. Learn. 33(1), 16–18 (2012)
  23. Naidoo, T., Kritzinger, E., Loock, M.: Cyber safety education: towards a cyber-safety awareness framework for primary schools. In: International Conference on e-Learning, p. 272. Academic Conferences International Limited (2013)
  24. Moreno, M.A., Egan, K.G., Bare, K., Young, H.N., Cox, E.D.: Internet safety education for youth: stakeholder perspectives. BMC Public Health 13(1), 543 (2013)
  25. Qustodio: Protect, understand and manage your kids internet activity with Qustodio (2016). <https://www.qustodio.com/en/>
  26. The Windows Club: SocialShield: Avira Social Network Protection for your child (2016). <http://www.thewindowsclub.com/socialshield-review>
  27. WOT: Know which sites to trust (2016). <https://www.mywot.com/>
  28. Awareness Technologies Computer & Mobile monitoring software (2016). <http://www.webwatcher.com/?refID=lnkshr&siteID=Cty0dj6o3sgGHtU.M9eT5Zlm7qQ5Ms1ig>
  29. Cloudacl: Web Security Service (2013). <http://www.cloudacl.com/webfilter/>
  30. Squicciarini, A.C., Dupont, J., Chen, R.: Online abusive users analytics through visualization. In: Proceedings of the 23rd International Conference on World Wide Web, pp. 155–158. ACM, April 2014
  31. Mozilla add-on: The Parental control for Firefox (2014). <https://addons.mozilla.org/en-US/firefox/addon/foxfilter/>
  32. Chrome web store: Parental Controls & and Web Filter (2016). <https://chrome.google.com/webstore/detail/parentalcontrols-web-fil/dpfbddcgbimoafpgmbbjiliekgkfcjkmn>
  33. MetaCert: MetaCert Security API (2009–2016). <https://metacert.com/>
  34. Esafely: eSafely protects you where your Web filter doesn’t (2014). <http://www.esafely.com/>
  35. ReThink: ReThink (2016). <http://www.rethinkwords.com/>
  36. Puresight: PureSight Online child safety (2010–2011). <http://puresight.com/puresight-prevents-cyberbullying.html>
  37. Pervasive Group: MM Guardian Parental Control (2016). <https://play.google.com/store/apps/details?id=com.mmguardian.childapp>
  38. Funamo: Funamo Parental Control (2015). <https://play.google.com/store/apps/details?id=funamo.funamo>
  39. General Solutions and Services, LLC: Kids Place - Parental Control (2012).

- <https://play.google.com/store/apps/details?id=com.kiddoware.kidsplace>
40. doMobile: AppLock (2016).  
<https://play.google.com/store/apps/details?id=com.domobile.applock>
41. ScreenTime Labs: Screen Time Parental Control (2016).  
[https://play.google.com/store/apps/details?id=com.screentime.rc&hl=en\\_GB](https://play.google.com/store/apps/details?id=com.screentime.rc&hl=en_GB)
42. O’Brien, D., Budish, R., Faris, R., Gasser, U., Lin, T.: Privacy and Cybersecurity Research Briefing (2016)

## 6. Discovering Social Bridges in Microblogs (study 4)

With the emerging and intense use of Online Social Networks (OSNs) amongst young children and teenagers (youngsters), safe networking and socializing on the Web has faced extensive scrutiny. Content and interactions which are considered safe for adult OSN users might embed potentially threatening and malicious information when it comes to underage users. The topology of a graph is studied towards detecting the so called “social bridges”, i.e. the major supporters of malicious users, who have links and ties to both honest and malicious user communities. A graph-topology based classification scheme is proposed to detect such bridge linkages which are suspicious for threatening youngsters networking. The proposed scheme is validated by a Twitter network, at which potentially dangerous users are identified based on their Twitter connections.

Malicious behavior on the Web has emerged in various internet applications including, but not limited to, email services, shopping and recommendation platforms, crowdsourcing websites, mashups and OSNs. Such behavior has heavily impacted popular and widely used OSN platforms and applications, since they are open and easily accessible large crowds forums, forming structures such as the social graph [72]. Therefore, social networks constitute a breeding ground for the spread of malicious behavioral patterns, like spamming, link farming, Sybil attacks (forged profile identities), phishing and the even more dangerous pedophile attacks, online grooming, etc. [73]. In this direction, the social network providers (Twitter, Instagram, Facebook, Flickr, YouTube, etc.), the authorities, as well as the scientific community, are invested in analyzing social media data and identifying or even predicting the aforementioned behavioral patterns. To this end, data from web-based communities and user generated content needs to be utilized, such as connections from social-networking sites, video sharing sites, blogs, folksonomies, etc.

In the context of the present study, we conducted an empirical analysis of the social dynamics of spam accounts in OSNs and the ways they form connections with the rest of the network to reach the honest users. The concept of spamming in OSNs and the ways to identify it have been extensively studied with approaches including automatic dissemination of spam like [74], tools used by spammers to deceive search engines [75] or faking honest behaviors [76].

Although these approaches are efficient and their prediction results seem promising, they do not attempt to identify all potentially dangerous users in real world networks. As it is often the case, spammers manage to mimic honest users' behavior and, by connecting with them, they penetrate the strongly connected component of a network making it challenging to identify them.

More specifically, we contemplated the social behavior these spam users display, to increase their impact. We expanded the concept of dangerous or malicious users in OSNs, beyond the obvious



spam accounts, to facilitate the needs of more sensitive OSN users, such as young adolescents and children. A motivating scenario would be a young child that makes a new connection in an OSN with a user that appears to be connected with other children from the same school or neighborhood. If this new user has not explicitly shared malicious content online, conventional detection systems would not provide an alert for this new connection and that might be justifiable for adult users. However, this might not suffice to protect a kid from exposure to inappropriate users. Should this new connection have links to spammers or generally malicious users, the child could be exposed to other far more dangerous new connections by entering a network part with criminal communities. A young user could also be faced with inappropriate shared content that is being spread in this network part. In this article we refer to the users that help link spammers to the core of the network as social bridges .

Various groups of users tend to follow criminal accounts (e.g. spam accounts), and they display certain identifiable behavioral patterns. In [77] criminal hubs and criminal leaves were identified as users that follow a large number of criminal accounts and the ones that have limited connections to the criminal communities respectively. A further categorization of the extracted criminal hubs was conducted by dividing them into social butterflies, social promoters and dummies. Each of these categories has different motives for following criminal accounts, either knowingly or not, and could prove being dangerous themselves. The spam-neighborhood has been contemplated in [78] and the spam followers have been found to be increasingly influential nodes in a network.

### 6.1. Social Bridges Detection:

Firstly, to identify the social dynamics of spammers and their followers we have isolated these groups and their followers. Second, we have extracted the connected components of this network part using the Tarjan algorithm (Tarjan, 1972) [79]. As shown in **Error! Reference source not found.**, there are three identified components presented with *black*, *red* and *green* nodes. Then, we calculated the percentages of spammers and their associated connections that belong to each component. The majority (92%) of the least populated component *black* is comprised of spam users, while the *red* component contains 87% spam followers. The biggest of the components is mainly (96%) populated with honest users whom the other two components follow. The graph center represents the largest connected component in this subset of the Twitter graph and the seemingly unpopular (disconnected) spam users (depicted on the bottom right of the figure with *black* use their connection to the second connected component *red* to penetrate the dense network center *green*). Therefore, these spam followers, constituting the majority of the second component, can be considered as a dangerous influence especially for the most vulnerable and impressionable users of the Twitter network (i.e. children) and constitute the social bridges of spammers. The group of spammers and social bridges will be referred to as malicious users.

To further analyze the different topological positioning of the malicious group in the Twitter graph as compared to the honest users, we have utilized a set of widely used network features [80]:

- **In-Degree** defined as the number of incoming connections (followers) a user has.
- **Out-Degree** defined as the number of users a node follows (outgoing connections).

- **Betweenness centrality** which is equal to the number of shortest paths from all users to all others that pass through that specific node (i.e. user). It is a metric indicative of a user's influence in a network. As previous studies have indicated, we have confirmed that the bridge users are highly influential nodes in a graph ranking high in betweenness centrality values.
- **Closeness centrality** which is the mean distance from a vertex to other vertices. For our Twitter graph, as it contained a number of disconnected nodes, we utilized the harmonic mean to calculate representative values for the closeness centrality. Nodes with a low value in this metric might have better access to information than other nodes or more direct influence on other users of the network.
- **Eigenvector centrality** is an extension of in-degree centrality that awards higher importance to links coming from more relevant nodes. In other words, a node is important (high eigenvector value) if it is linked to other important nodes.

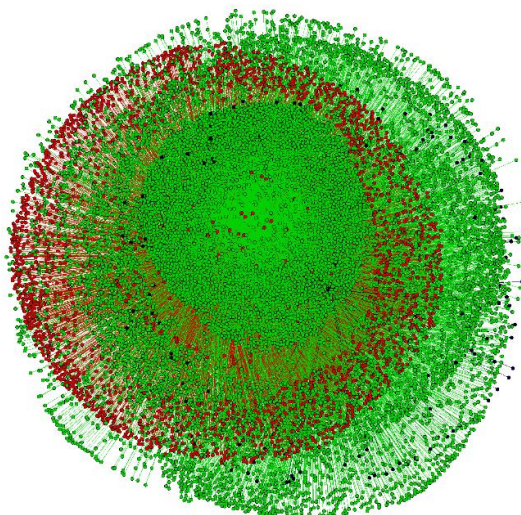


Figure 4. A subsample of Twitter user graph including the followers of spammers (SF) and the SF's followers. Three different components are identified depicted in black, red and green

- **K-core** number is defined as the largest integer  $k$  for a node such that this node exists in a graph where all vertices have degree  $\geq k$  [Seidman1983]. Usually, the nodes belonging to the highest  $k$ -core ( $k_{max}$ ) comprise a well-connected globally distributed subset of the network, identified as the *nucleus* in an analogous study on linkage between web-pages [Carmi2007]. In the case of Twitter users, the  $k_{max}$  core comprises of 72% malicious users and 28% of honest users. This is a surprising finding indicating that particularly the social bridges are often well connected users that can influence a large network part. This justifies the spammers tendency to attach to them to approach the majority of honest users. The largest connected component of the  $k_{max} - 1$  shell (the second largest  $k$ -core) constitutes the *peer-component* (as named in [Carmi2007]), which is the most well-connected

component of the majority of users that remains connected even when we remove the  $k_{max}$  group. The 88% of the peer-component is comprised of honest users and the remaining percentage represents the malicious users. The rest of the graph contains low-connected users that would become entirely disconnected, if the peer-component and  $k_{max}$  were removed.

In Figure 3 we have summarized the percentage differences of the network features discussed above for the three identified user categories. The differences are calculated as:

$$DF(\%) = \frac{mean(group1) - mean(group2)}{mean(group2)}$$

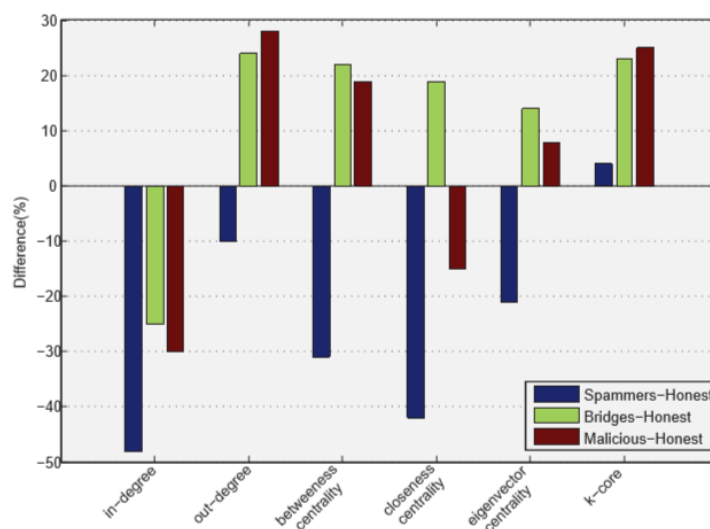
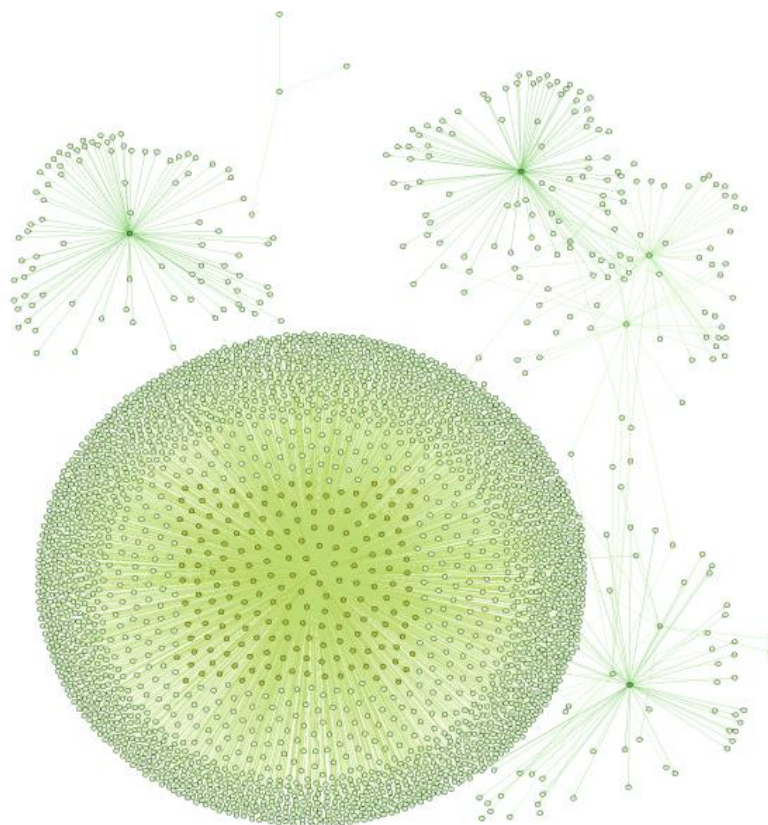


Figure 5. Bar chart of the percentage differences for the 6 networks features amongst the 3 identified user groups

We observe that the values of in-degree and closeness centrality are lower for spammers as compared to honest users. The social bridges display all the characteristics of influential users with high centralities, as discussed above. In addition, the social bridges display similarities with both honest users and spammers in their topological features.

**Error! Reference source not found.** depicts a subsample of spammers and the users they follow, but the social bridges have been removed. Consequently, the spam nodes become severely disconnected from the major connected component. It comes out that, when the bridge users are removed from the spammers' connections they lose their access to the network core, in the sense that the users they manage to connect to are not central influential nodes. As a result, it becomes challenging for them to increase their connections and their impact. This observation indicates the dangers innocent users face when connecting with the social bridges; they become part of the expansive network of malicious users increasing the probability of connecting with the criminals (spammers) themselves.

A new category of influential Twitter users is identified and associated with malicious behavior across the Twitter user graph. The different behavioral patterns of these two categories of users that pose dangers to particularly vulnerable groups of users (such as children) and their intrinsic characteristics are explored to allow for alerts to occur when a new connection is added. In the future, we plan to expand the features used to include semantic or textual information and apply our best performing classification scheme to other OSNs, as well.



**Figure 6. A subset of Twitter user graph including a set of spammer users (isolated nodes) and the users they follow, excluding social bridges. The major connected component is depicted in the center**

## 7. Survey of use of OSNs by minors (study 5)

### 7.1. Study of previous research with similar surveys

The main tool to study minors, their usage on OSNs and their impressions about security and privacy was a survey. For the purposes of our work, we studied selected surveys from previous similar studies closed to our task. The keywords of this research were: *teenagers and OSNs*, *security on the web*, *privacy on the internet* and *sensitive content*. Studying these subjects help us to identify and notice down appropriate questions about these issues. These questions were put in a row mixed with our new specific questions, in this way we develop the design of the survey. Moreover, some questions from other previous surveys added after modifying them to serve our research purposes. Similar international studies in the past and surveys we studied were helpful to notice selected questions for our survey design, these studies are accessible online [90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100].

### 7.2. Survey Design

Looking at past surveys a first draft of the survey was developed that was then pilot tested to help us fix any errors. A small number of students participated in the pilot tests. After these tests, some questions were rephrased and some others that were deemed as unnecessary were removed.

The structure of the survey contains at the beginning a small section for demographics details, and then three main parts. Part A is based on security and privacy on the internet (general), part B is about security/privacy of OSN and sensitive content, and finally part C is about opinions for an implicit protection of sensitive content on OSNs. The final survey was available in two versions, in a printed version and an online version in the form of an online web form.

### 7.3. Participants

Participants had to be minors (ages 12-17) users of at least one online social network account. The total number of participation was 76 minors. We had as a goal to keep a balance in participation between the two genders in the countries where the study run. Greece, Cyprus and United Kingdom were the three countries where this research took place.

### 7.4. Data Collection

The data were collected by filling the printed survey or answering it through the online form (Google Form). We collected data from a random sample of 76 minors, users of online social networks. The participants before answering the questionnaire gave their verbal consent to participate in the study. The questionnaire could be completed in about 8-15 minutes. After the data collection was completed, we gathered all the results in the main google form to analyse them.

## 7.5. Survey Results

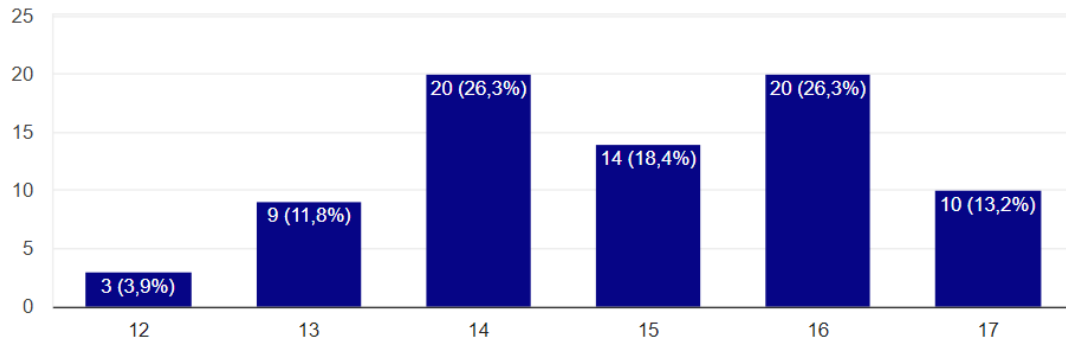


Figure 7. Age distribution of participants



Figure 8. Results diagram for Ques. 1, from survey Part A:  
In general, how concerned are you about security on the Internet? (e.g people reading your email, finding out what websites you visit, etc.)

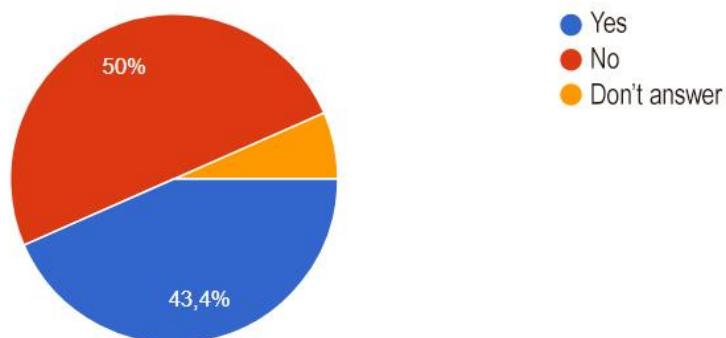


Figure 9. Results diagram for Ques. 2, from survey Part A:  
Are you willing to use your credit card on the web?

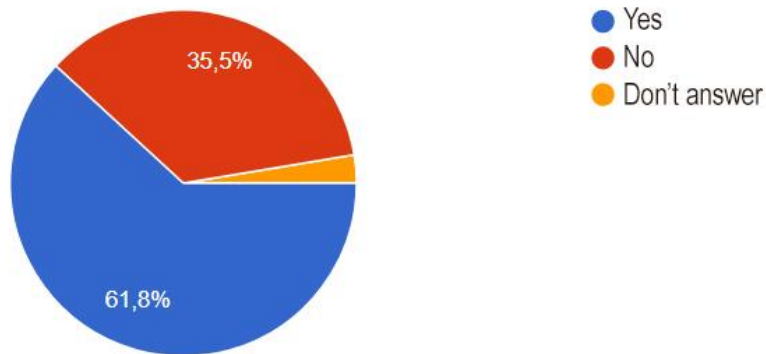


Figure 10. Results Diagram for Ques. 3, from survey Part A:  
 Do you buy online?

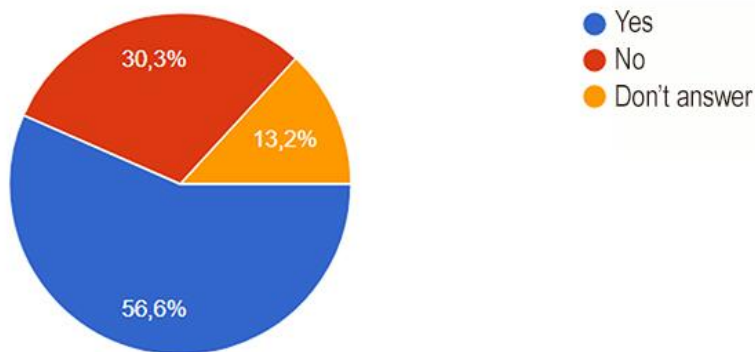


Figure 11. Results Diagram for Ques. 4, from survey Part A:  
 Do you think rating on how "secure" is one specific website is it helpful or have any value to you?

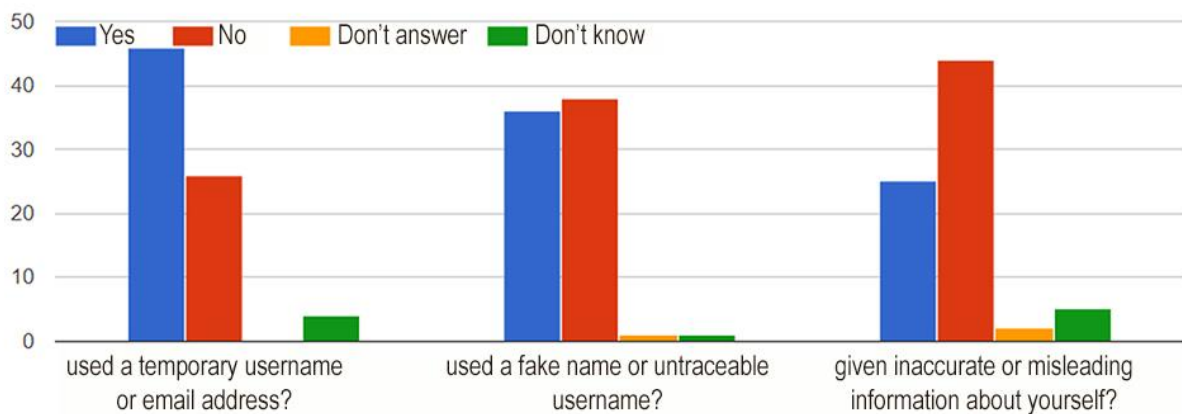
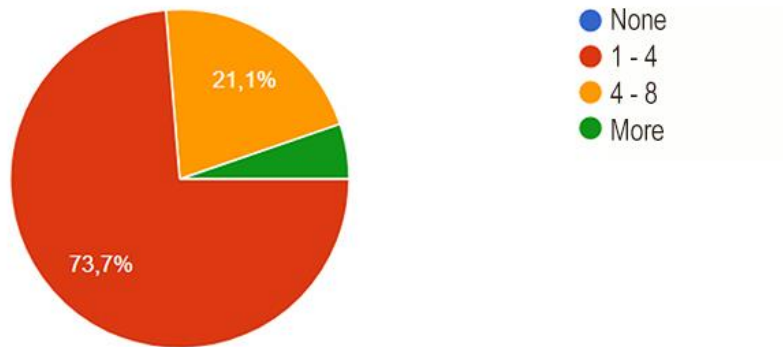
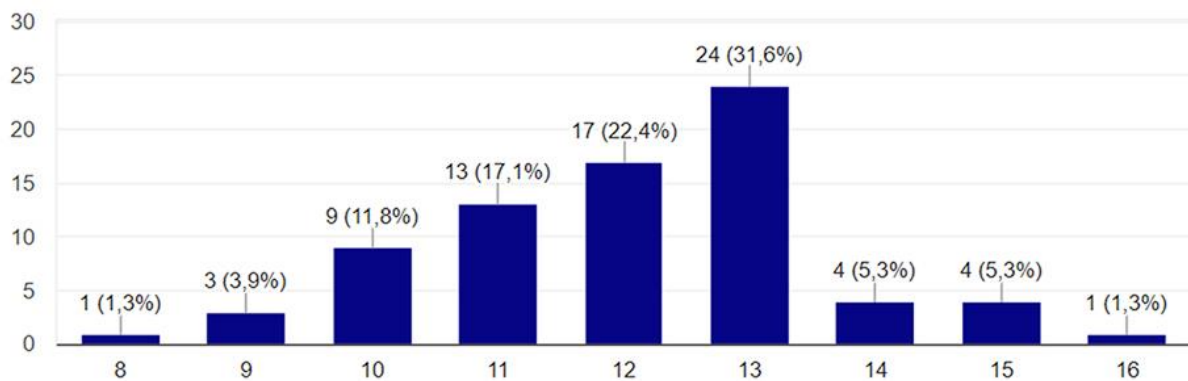


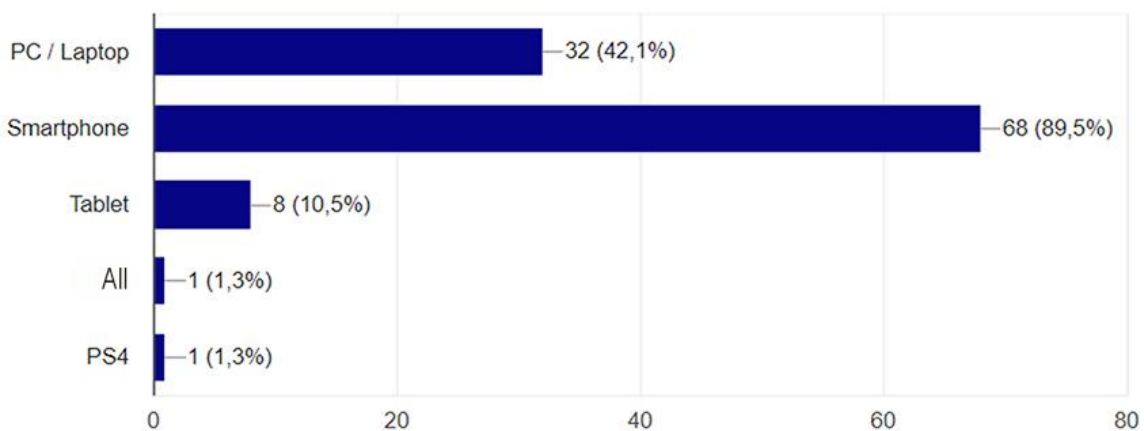
Figure 12. Results Diagram for Ques. 5, from survey Part A:  
 While using the internet, have you ever done any of the following things? Have you ever [a, b & c] while you used the internet:



**Figure 13. Results Diagram for Ques. 2, from survey Part B:**  
 How many social networking sites / communities / are you a member of?

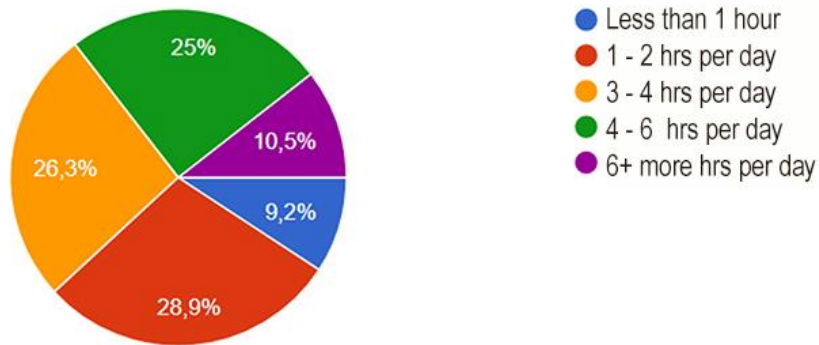


**Figure 14. Results Diagram for Ques. 3, from survey Part B:**  
 Your age when for a first time you join a social network.

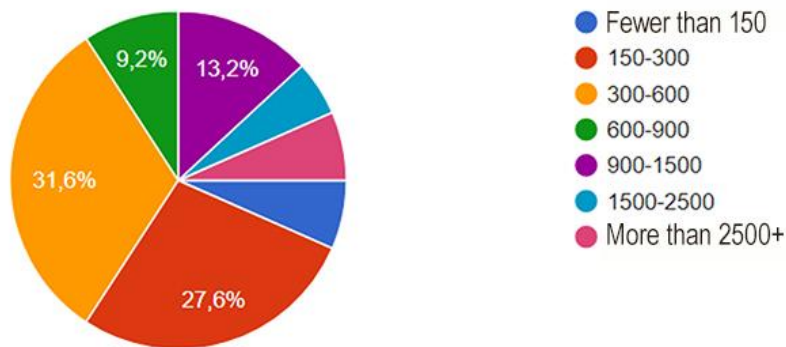


**Figure 15. Results Diagram for Ques. 4, from survey Part B:**  
 Usually, how do you access your social network account?

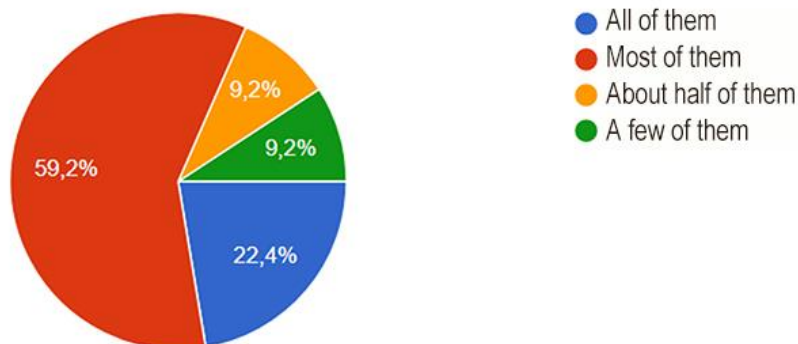




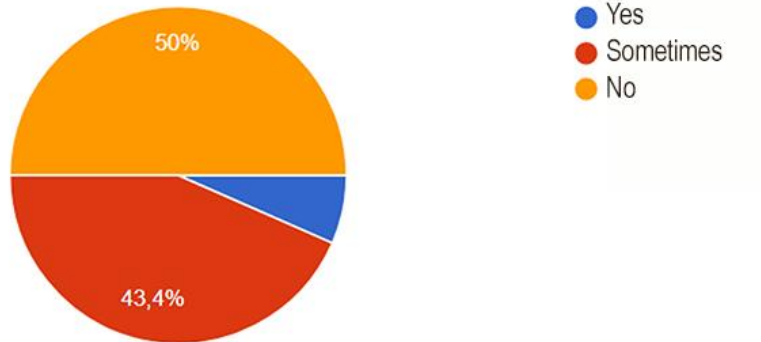
**Figure 16. Results Diagram for Ques. 5, from survey Part B:**  
 On average, how much time do you spend daily on social networking sites?



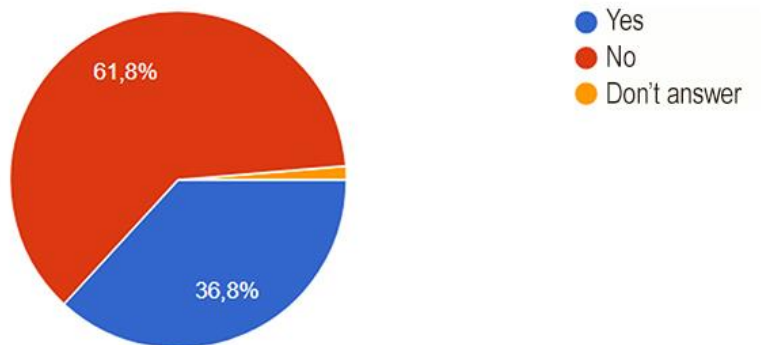
**Figure 17. Results Diagram for Ques. 6, from survey Part B:**  
 How many contacts/friends do you have in total in all of your social networks sites?



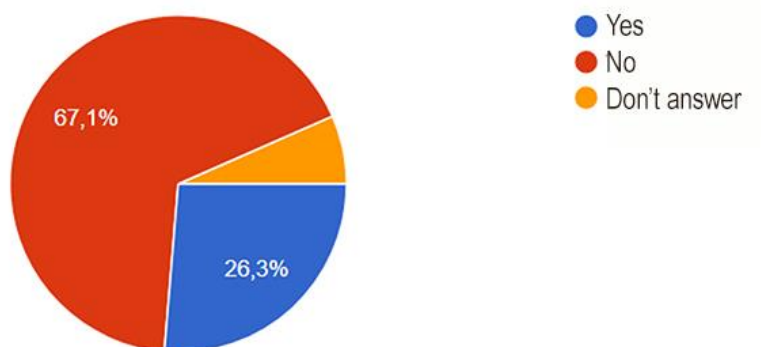
**Figure 18. Results Diagram for Ques. 7, from survey Part B:**  
 About how many of your friends on your social networks sites do you consider that you know them?



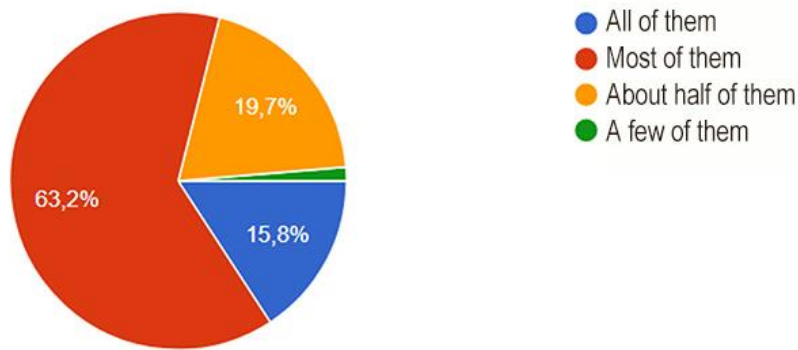
**Figure 19. Results Diagram for Ques. 8, from survey Part B:**  
 Do you accept friend requests / or follow request from strangers who in social network sites?



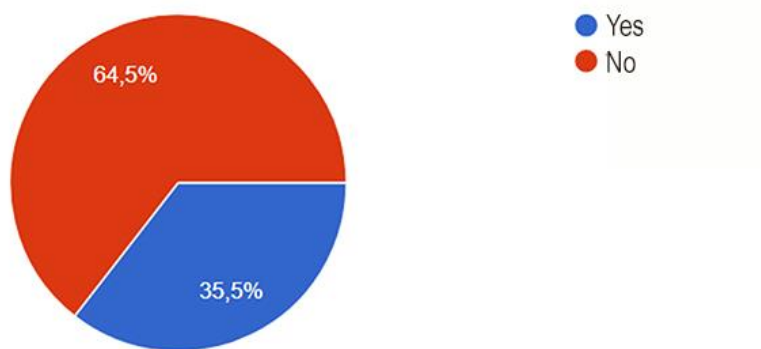
**Figure 20. Results Diagram for Ques. 9, from survey Part B:**  
 Have you ever met with somebody (you didn't know personally before) after chatting through a social network site?



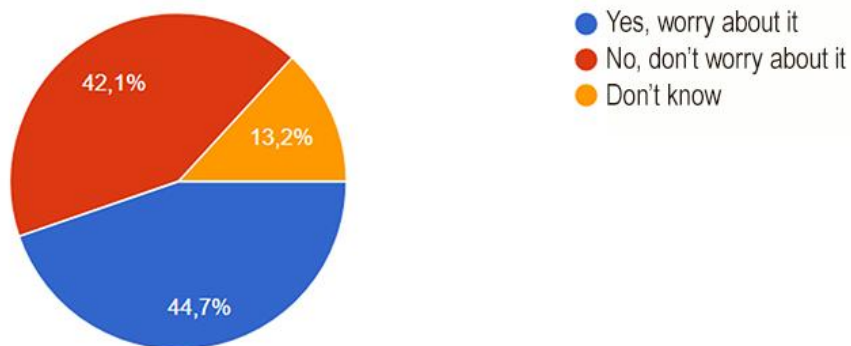
**Figure 21. Results Diagram for Ques. 10, from survey Part B:**  
 Would you trust random strangers to view your profile?



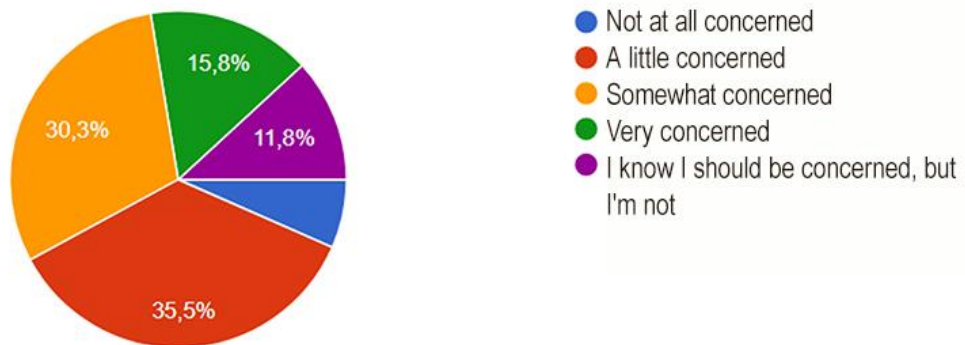
**Figure 22. Results Diagram for Ques. 11, from survey Part B:**  
 Do you trust all your connected friends with all parts of your profile?



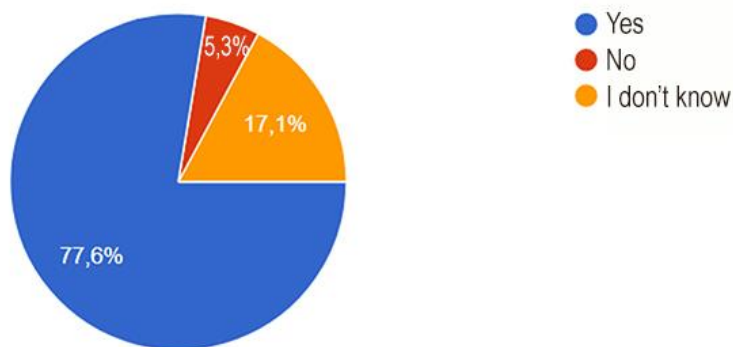
**Figure 23. Results Diagram for Ques. 12, from survey Part B**  
 Are you “connected” with stranger “friends” from abroad on your social network accounts?



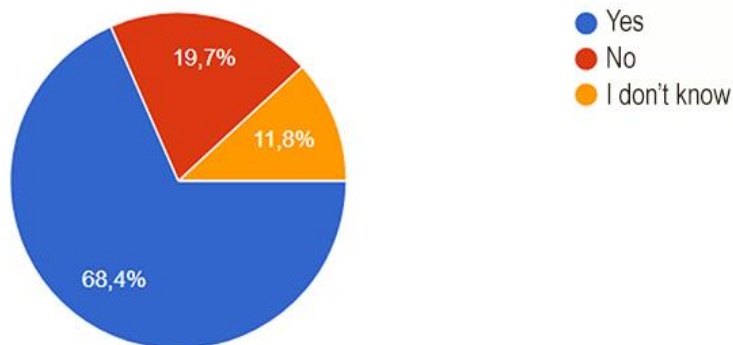
**Figure 24. Results Diagram for Ques. 13, from survey Part B:**  
 Do you ever worry about how much information is available about you on the internet, or is that not something you worry about?



**Figure 25. Results Diagram for Ques. 14, from survey Part B:**  
**How concerned are you about your security and privacy of your sensitive content (personal information) on your social networks?**



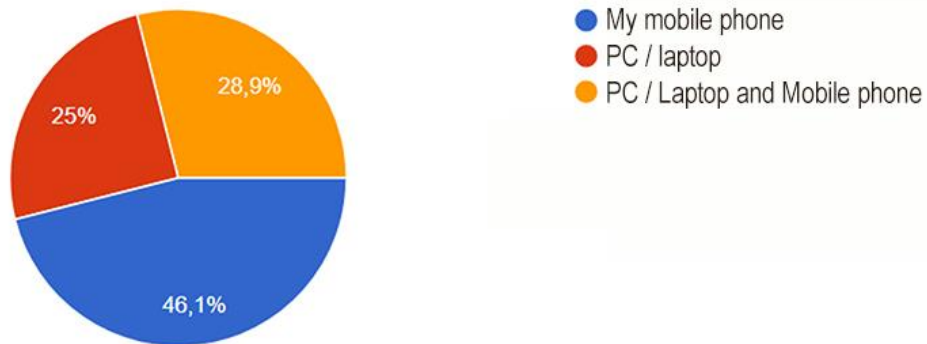
**Figure 26. Results Diagram for Ques. 15, from survey Part B:**  
**Are you interested in controlling the privacy settings of your account?**



**Figure 27. Results Diagram for Ques. 16, from survey Part B:**  
**Have you changed the privacy settings of your account/s?**



**Figure 28. Results Diagram for Ques. 17, from survey Part B:**  
 How do you control the privacy settings of your social media accounts? Select the most valid for you



**Figure 29. Results Diagram for Ques. 18, from survey Part B:**  
 What device you use to change the privacy settings?

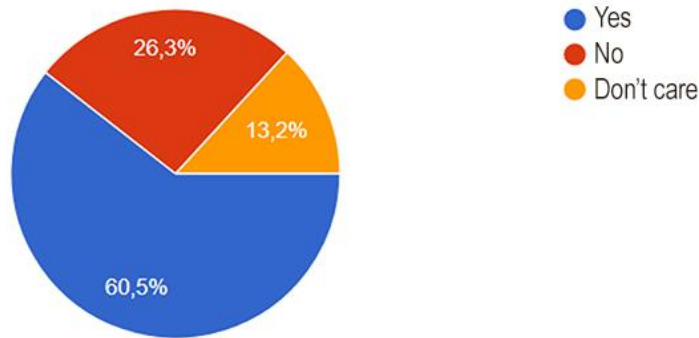


Figure 30. Results Diagram for Ques. 21, from survey Part B:

Do you think controlling access of certain content on your profile is necessary in your accounts on online social networks?

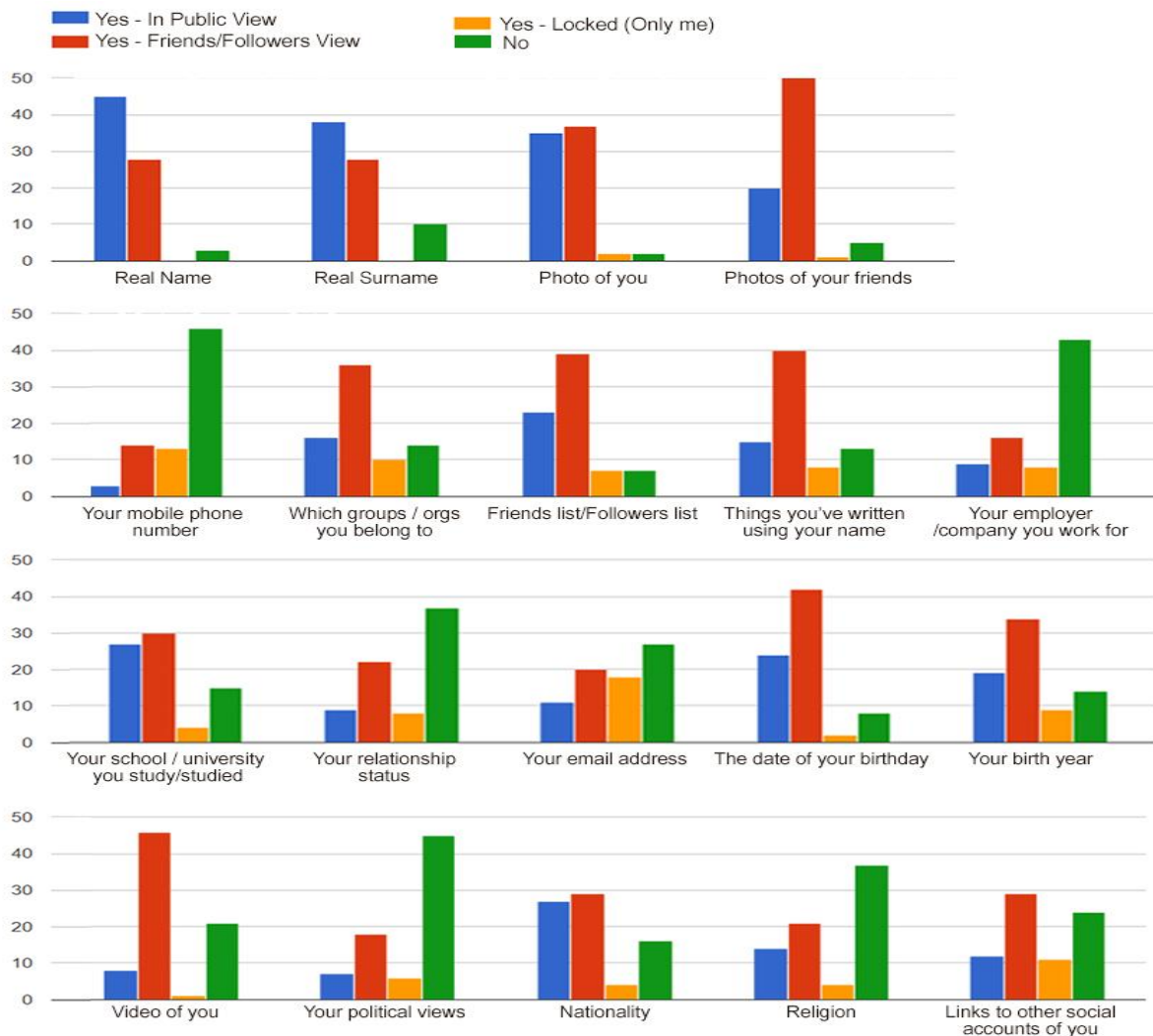
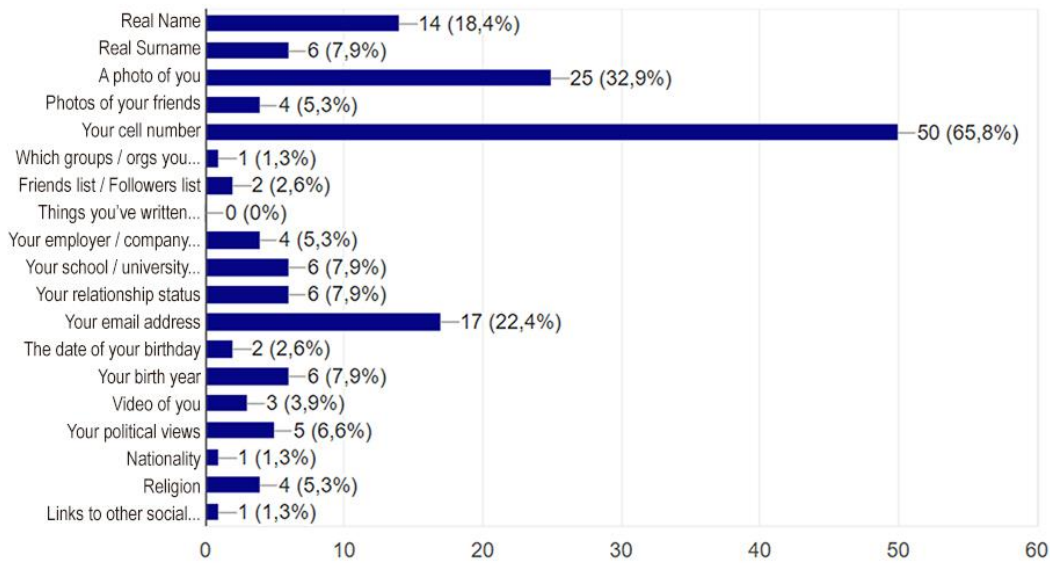
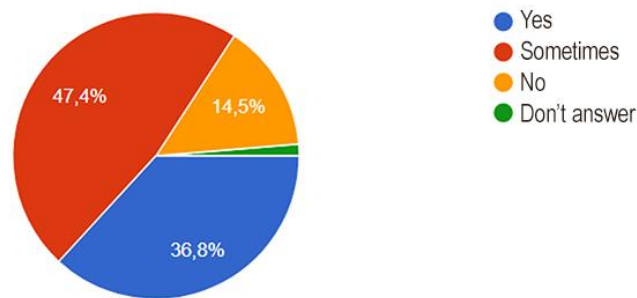


Figure 31. Results Diagram for Ques. 19, from survey Part B:

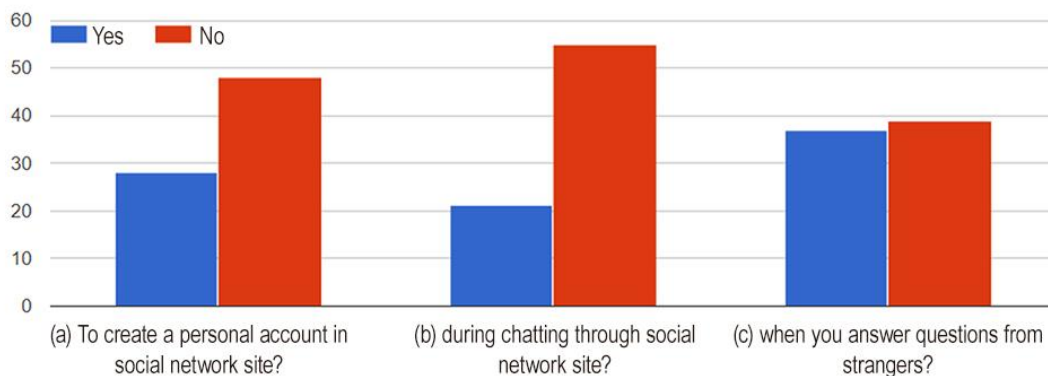
Please indicate if now online you provide the following information for yourself in one of your social accounts (If Yes please select in which privacy settings provided)



**Figure 32. Results Diagram for Ques. 20, from survey Part B:**  
Please note at least 1 (to 3) personal details, which you perceive them as important sensitive content for yourself



**Figure 33. Results Diagram for Ques. 22, from survey Part B:**  
Do you think you can recognize a fake account?



**Figure 34. Results Diagram for Ques. 23, from survey Part B:**  
Have you ever provide fake personal details: (a), (b), (c)

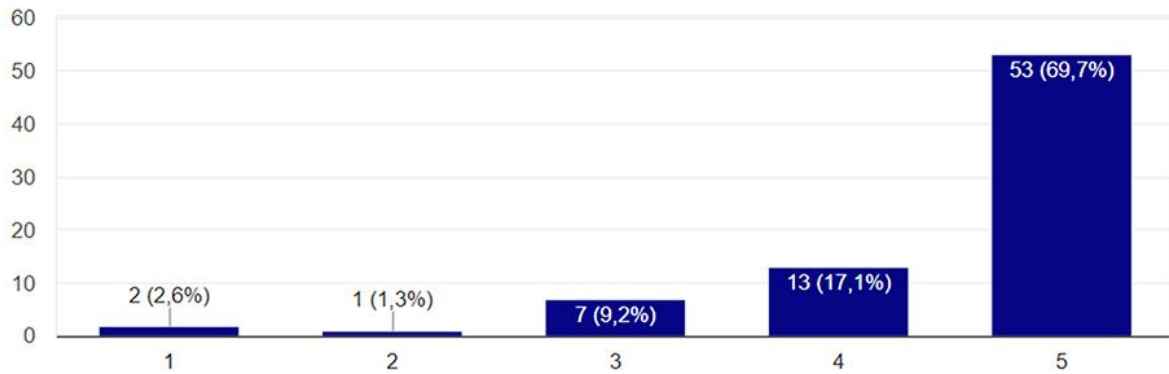


Figure 35. Results Diagram for Ques. 24(a), from survey Part B:

Please note the if you agree or not with the following statements: Please choose from a scale of 1 to 5 (1: Strongly Disagree / 2: Disagree / 3: Maybe / 4: Agree / 5: Strongly agree) “I understand that there are dangerous people in social network sites

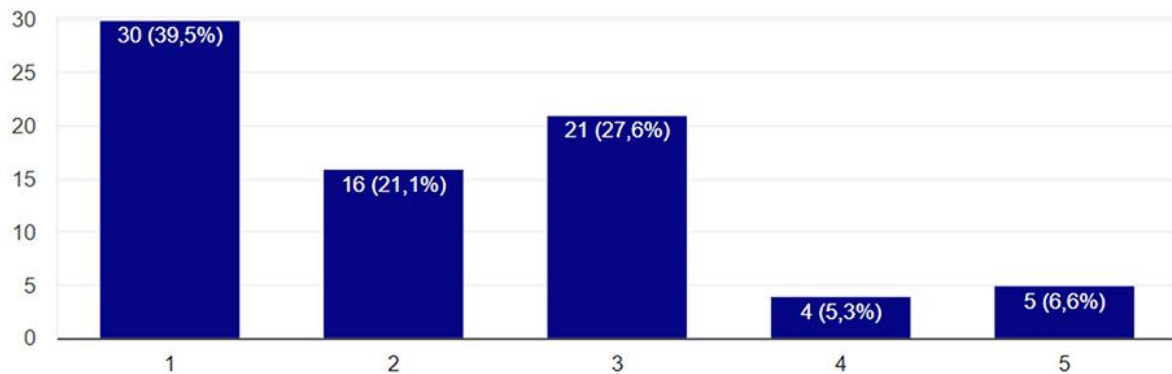


Figure 36. Results Diagram for Ques. 24(b), from survey Part B:

“I don’t believe that there are dangers if the stranger ‘friend’ lives abroad”

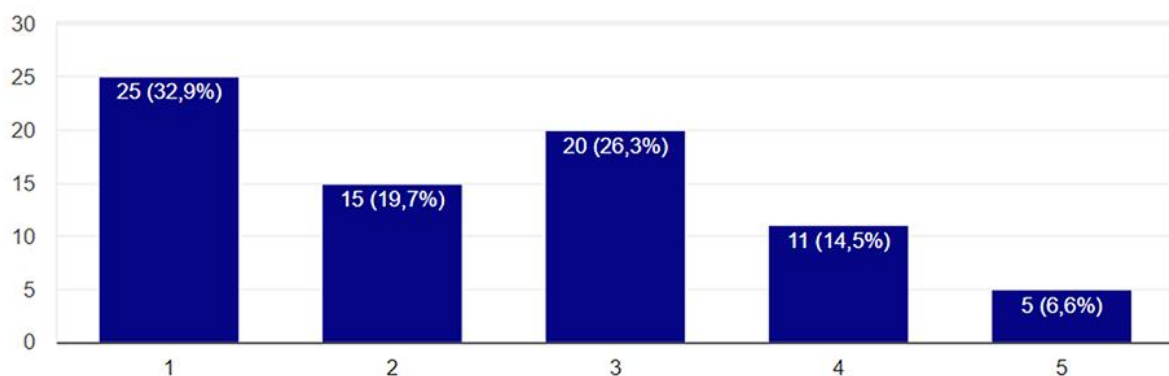
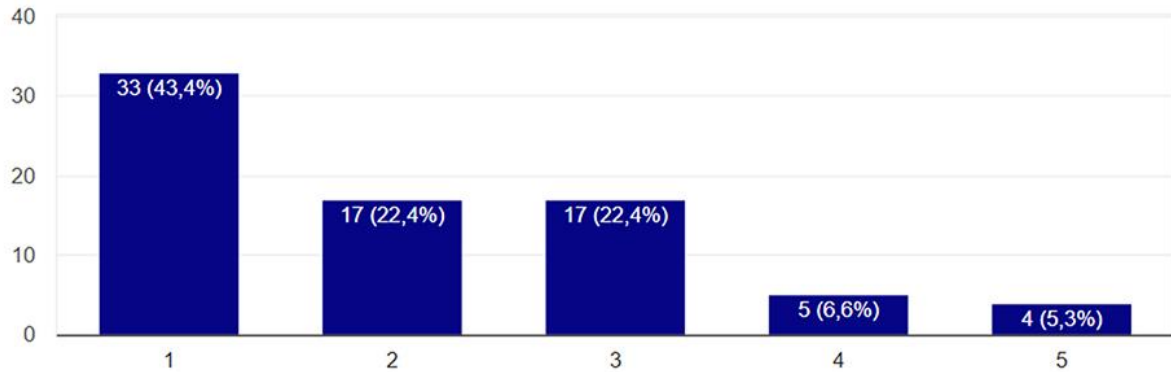


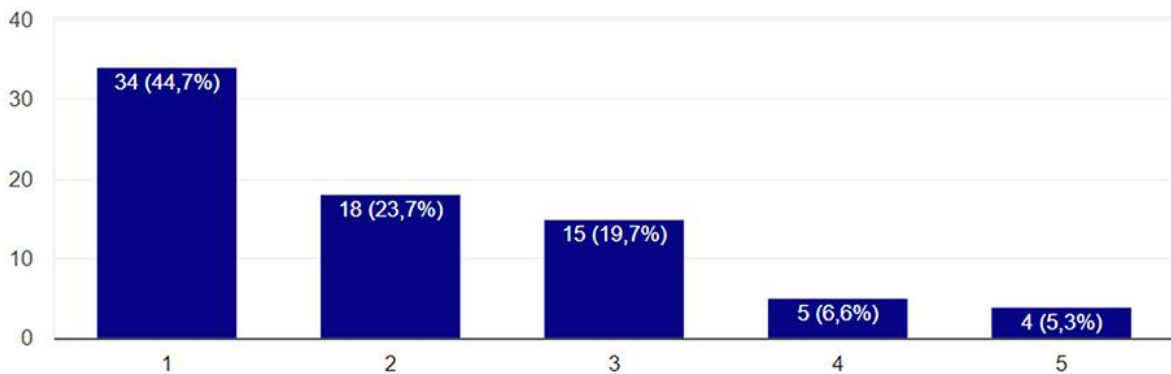
Figure 37. Results Diagram for Ques. 24(c), from survey Part B:

“The nationality of the stranger “friend” affects me to what way I can interact with him/her”

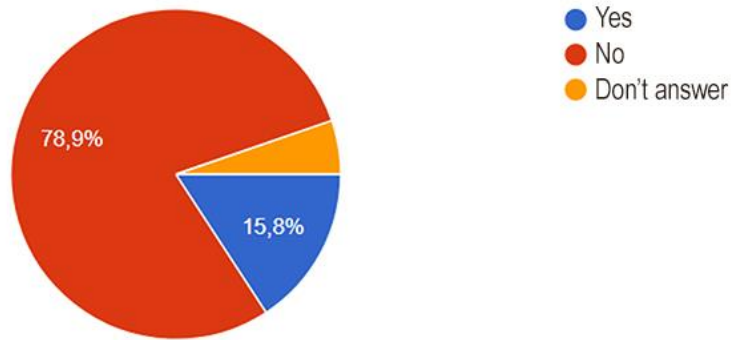




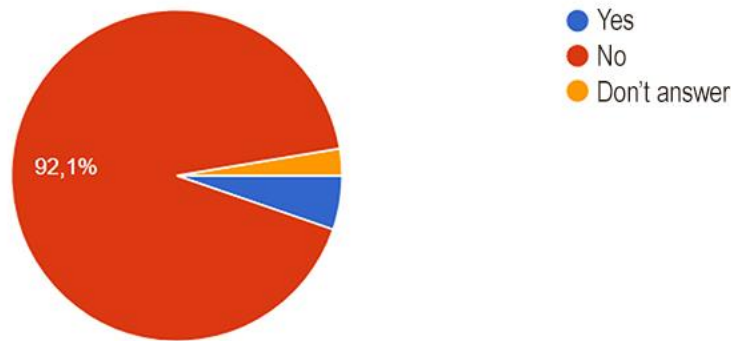
**Figure 38. Results Diagram for Ques. 24(d), from survey Part B:**  
**"During chatting in social network site If a local "friend" asked me to provide some personal details, maybe I would do it."**



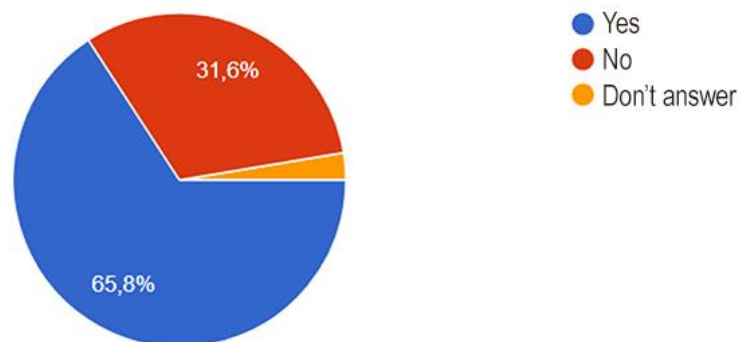
**Figure 39. Results Diagram for Ques. 24(e), from survey Part B:**  
**"During chatting in social network site If a "friend" from abroad asked me to provide some personal details, maybe I would do it."**



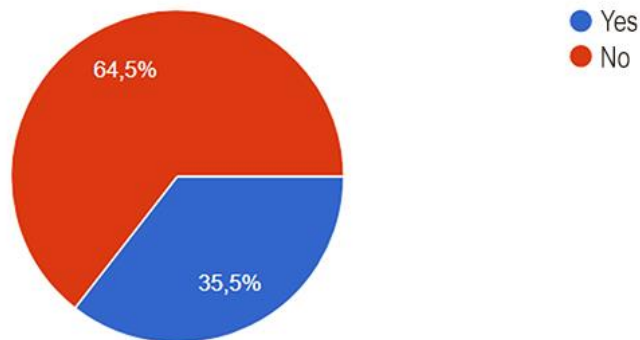
**Figure 40. Results Diagram for Ques. 25, from survey Part B:**  
 During your experience in social networks have you ever found yourself to be faced with a cyber bullying?



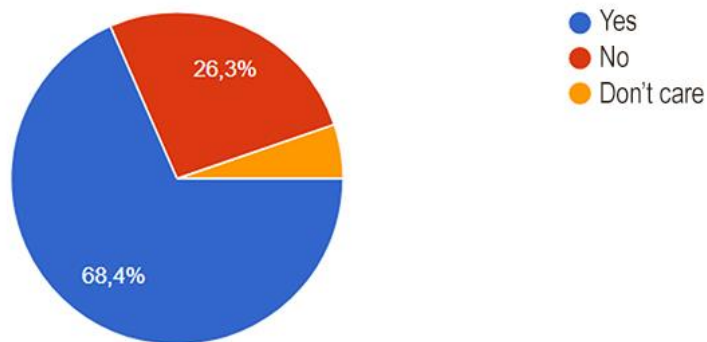
**Figure 41. Results Diagram for Ques. 26, from survey Part B:**  
 During your experience in social networks have you ever found yourself to be faced with the threat sexual abuse in your private life?



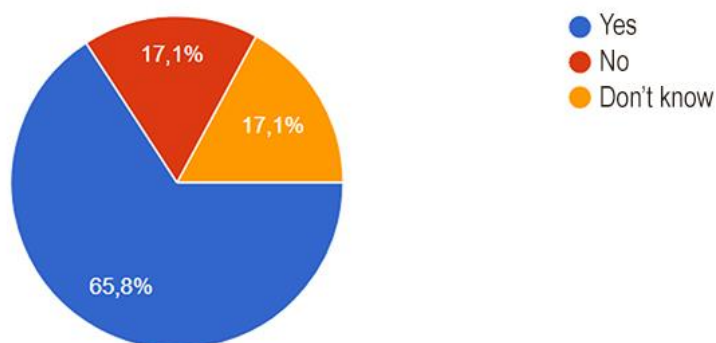
**Figure 42. Results Diagram for Ques. 27, from survey Part B:**  
 Have you ever “fight” with somebody other user on your social network account?  
 (e.g. during chatting, or in comments on a post)



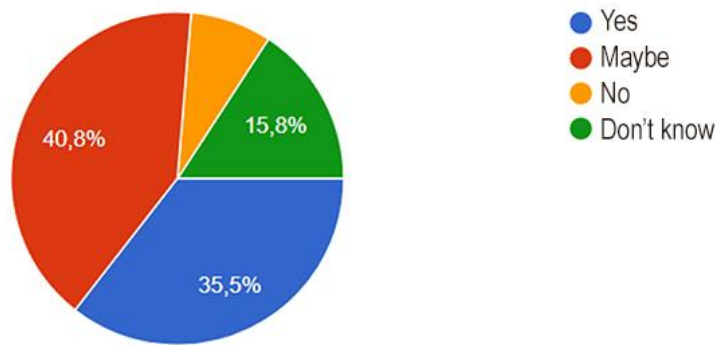
**Figure 43. Results Diagram for Ques. 28, from survey Part B:**  
 Through your experience on social networks have you ever feel that you are in danger in some way?



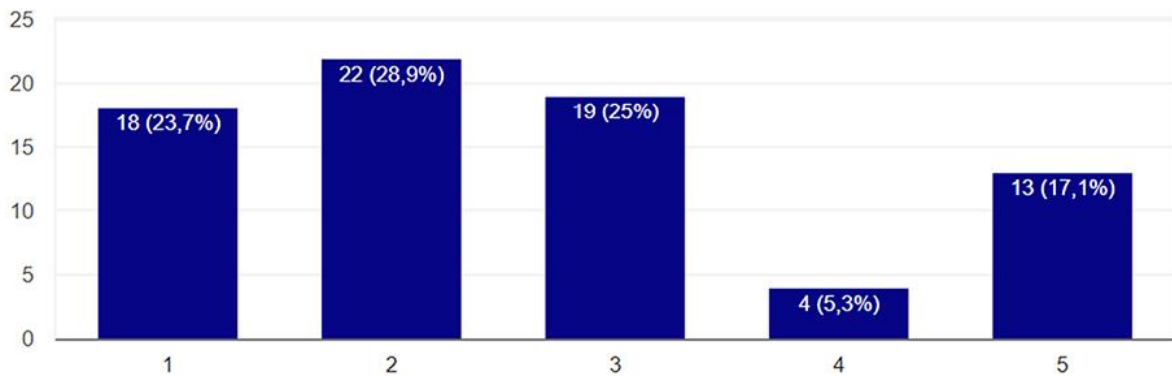
**Figure 44. Results Diagram for Ques. 1, from survey Part C:**  
 Are you satisfied with current privacy controls methods?



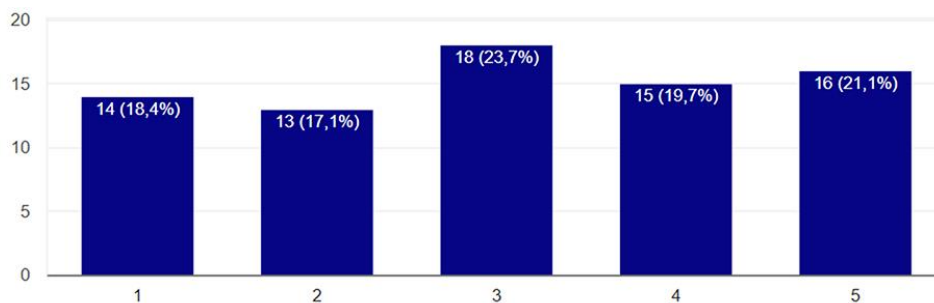
**Figure 45. Results Diagram for Ques. 2, from survey Part C:**  
 Would you prefer more advanced settings to protect your privacy on online social networks?



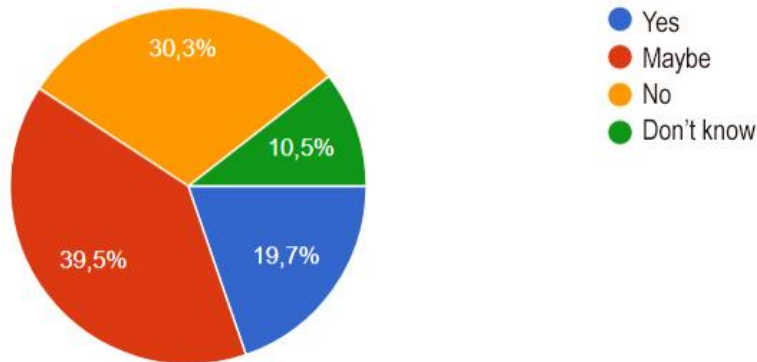
**Figure 46. Results Diagram for Ques. 3, from survey Part C:**  
 Would you be eager to provide individual characteristics to protect your personal data online?



**Figure 47. Results Diagram for Ques. 4(a), from survey Part C:**  
 If a new tool applied on your social networks accounts with a goal of an implicit protection of your sensitive content information, how acceptable are you to provide to the system characteristics such as: (a) your face scan? 1: Strongly Disagree / 2: Disagree / 3: Maybe / 4: Agree / 5: Strongly agree)



**Figure 48. Results Diagram for Ques. 4(b), from survey Part C:**  
 If a new tool applied on your social networks accounts with a goal of an implicit protection of your sensitive content information, how acceptable are you to provide to the system characteristics such as: (b) your finger prints?



**Figure 49. Results Diagram for Ques. 5, from survey Part C:**  
**Do you think you would feel more protected if you provide these characteristics?**

## 7.6. Discussion on Findings

Below we provide the main findings of our survey study:

- 62% of the participants buy online, only 43% are willing to use their own credit card for that.
- The majority of teenager participating in the survey are members of 1 to 4 social networks
- 1 minor out of 5 maintains more than four different social network accounts and 1 out of 10 maintains 8 or more social network accounts
- They first joined an online social network in the age of 10 to 13 (Small percent of 5% has joined a social network at the age of 8 and 9 years old)
- The majority of the participants don't worry about how much information is available about them on the internet
- According to the findings, it seems that generally they appear to be concerned the security and privacy of their sensitive content in their accounts
- 68% had changed their privacy settings in their OSNs account/s
- Most of them (66%) would prefer more advanced settings to protect their privacy on OSNs
- Half of the minors accept friend requests / or follow request from strangers on OSNs
- 2 out of 5 had met with somebody (who they didn't know personally before) after chatting through an OSN site
- 8 out of 10 don't trust all their connected friends with all parts of their profile
- They consider their phone number (66%), a photo of them (33%), their email (22%) and their real name (18%) perceived as most important sensitive content for their self from all personal details that they shared online
- Almost 40% of the participants during their experience in online social networks had felt that they were in danger in some way
- Majority are willing to provide some personal characteristics to a system for their security

Below we provide our findings related to Usability (Expectations / Needs / Concerns)

**How minors access their social network account:** Most participants (89.5%) use their smartphones to access their social network accounts, second option is the use of laptop or PC (42.5%), and third option tablet (with 10.5%).

**How much time they spend daily on OSNs:** Usually they spend daily 1 to 6 hours on their social network accounts. A percentage of 28.9% answered 1-2 hours, 26.3% answered 3-4 hours, 25% 4-6 hours and a small percentage 10.5% spends daily more than 6 hours.

**How they control their privacy settings:** Most teenagers had changed their default privacy settings on their accounts, they adjusted their privacy settings to control who has access to what I publish on my account (82.9%). 10.5% stated that they don't really care to change it and 6.6% are not sure how they can control their privacy settings.

**Devices they used to change the privacy settings:** They change their privacy settings usually using their smartphone (46.1%), second option (28.9%) was smartphone and laptop (both) and 1 to 4 (25%) use laptop / PC.

**Findings related to: Security and Privacy (Expectations / Needs / Concerns):**

**Worry or not about how much information is available about them on the internet:** Almost half of them worry (44.7%) and the other half doesn't worry (42.1%). 13.2% answered “Don't know”.

**How many of their friends on OSNs consider that they know them:** The majority believes that they know their online friends. 59.2% answered that they know most of their online friends. 22.4% know all their connected friends, and a small percentage of 9.2% knows about half of them or fewer of them.

**Most important sensitive content for them:** In an open question where they were asked to note up to 3 personal details which they perceive as important sensitive content for their selves, 1<sup>st</sup> preference was their personal telephone number (65.8%), 2<sup>nd</sup> a photo of them (32.9%), and 3<sup>rd</sup> one personal email (22.4%). Interesting was also the fourth answer (18.4%) that they perceive their real name as important sensitive content. It seems that some teenagers don't like providing their real name on their online accounts.

**Recognize a fake account:** The majority, 47.4%, believes that sometimes they can recognize a fake online profile, 36,8% believes that they can always do this, and 14.5% they can't recognize it at all.

**Understand the existence of dangerous people (users) on OSNs:** From the results of a likert scale question, it seems that they know, and they agree with a statement that there are dangerous people in social network sites. 69.7% answered “Strongly agree”, and 17.1% “Agree”.

**Faced with a cyber bullying threat sexual abuse or in danger in some way:** Each participant was asked: (a) if he/she faced Cyber bullying – with results 78.9% “No”, 15.8% “Yes”, 5.3% “Don't answer”, (b) if he/she had ever found himself/herself to be faced with the threat of sexual abuse in

his/her private life – with results 92.1% “No”, 5.3% “Yes”, 2.6% “Don’t answer”, and last (c) if he/she ever felt to be in danger in some way – with results 64.5% “No”, and 35.5% “Yes”.

**Satisfied or not with current privacy controls methods:** 68.4% answered that their are satisfied with current privacy control methods, 26.3% answered negative. Despite the high present who answered that they are satisfy, it seems that most of them would prefer more options in the settings of such systems.

**Eager or not to provide individual characteristics to protect their personal data online:** From the results it seems that they are eager to provide some of their individual characteristics for a better protection online (40.8% “Maybe”, 35.5% “Yes”, 15.8% “Don’t know”, 7.9% “No”).

**They feel more protected or not if they provide these characteristics:** Yes most of them believe they will feel more protected if they provide these characteristics (39.5% answered “Maybe”, 19.7% answered “Yes”, 30.3% answered “No” and 10.5% “Don’t know”).

## 8. Usability Evaluation of Fraud Detection Systems (study 6)

This section provides a review of exciting security and fraud detection systems relevant to the concepts of ENCASE. A list of these web-based tools and mobile applications was provided in the Deliverable D2.2 of ENCASE with title “System Requirements and Software Architecture” in section 2.2 (page 13) [82].

### 8.1. Existing Security and Fraud Detection Systems

The exciting tools are mainly parental controls systems, (software, add-ons or mobile applications) with a common feature that they offer a more secure web browsing by blocking dangerous sites and other adult sites. Some of them have some function also about the security and privacy issues when using OSNs. Noticed that most of them are free for use and some others have free and pay edition (some of them only free trial version for a few days). Here is an overview of the capabilities of the studied tools:

**Qustodio** is parental control software available in most of the platforms [83]. It enables parents to monitor and manage their kids’ web and offline activity. It also allows them to track with whom their children are communicating within OSNs and manage their whole OSN activity. In addition, Qustodio can be used as a sensitive content detection and protection tool.

**WebWatcher** is a parental control, cross-platform compatible, monitoring software [84]. It is able to capture the content of emails and instant messages in OSNs, as well as actual keystrokes and screenshots. It assists parents in keeping their children safe online by viewing what is captured in their child’s screen from everywhere.

**PureSight** is a monitoring and filtering cross-platform software that allows children to use the internet without fearing bullies or harassment and keeps parents in the know [85]. It features

cyberbullying protection on Facebook, Web filtering, Reports and alerts, file sharing control and parent portal.

**TinyFilter Pro** is a web content filtering application which monitors browser activities and blocks inappropriate or offensive content. The extension helps users customize his filtering preferences and sensitivity settings so that any inappropriate or offensive content is filtered (add keywords to block websites) [86].

**FoxFilter** Parental control for Firefox is a free browser add-on produced by Mozilla and is known as the parental control for Firefox browser [87]. It is a personal content filter that helps blocking pornographic and other inappropriate content. A user can block content for an entire site or enter custom keywords that will be used to block content for any site that contains those keywords.

**MetaCert** is a parental control browser add-on that blocks pornography, malware and spyware [88]. It protects kids and adults across multiple categories. It allows you to choose among two main categories (extra strong for kids and Strong for adults) while also allows you to define the specific categories that you prefer to be protected (such as Bullying, Drugs, Aggressive behaviour, Gambling, Sex etc.).

**eSafely** is a parental control browser add-on that provides kid-safe access to popular web resources, free of adult content [89]. Generally, it offers the following: a) Kid Safe Facebook that protects children against cyberbullying by replacing harassing messages with friendly icons in Facebook chat; b) Kid Safe Images that when a site is identified as hosting adult content it replaces the images with images more suitable for children; c) Kid Safe YouTube; and d) Kid Safe Search \*eSafely add on does not support the 2nd capability of content Blocking

## 8.2. Methodology

After reviewing and selecting the tools, we focused on evaluating their usability. The methodology strategy was based on observation with basic research tools an eye tracker and a small survey.

Eye tracker can follow and track the eyes movements on the screen while the participant performs a task that was requested from them to complete. We had ready one experiment scenario with a simple task for the user / participant to try to execute it on a desktop computer. Using the eye tracker capabilities we captured useful data from every participant on how they managed to succeed to complete his/her task and by how much ease.

Three tools were selected for eye tracking experiments. These tools were selected as they were considered to be more relevant to the ENCASE future add-ons.. An extra reason to choose these tools is that are available for free use and easy installation, parameters that helped to organize the experiments better.

Part of the methodology study was to look online for reviews about these 3 selected tools and notice any important points of their disadvantages and any interesting suggestions from users. The software that were chosen for the purposes of the experperiments were:



1. Tiny Web Filter Pro
2. Qustodio
3. MetaCert

#### Various weaknesses identified by users

1. *“The extension does not filter keywords that are defined in non-English languages”* (for Tiny Web Filter Pro, [86]).
2. *“Password showing and not hidden: When its asking for my password the letters are not hidden with black dots its actually showing. Little bit tough keeping the password a secret from my kids this way”* (for Tiny Web Filter Pro, [86]).
3. *“I forgot password and cannot access the extension... You need a way to reset password if the user forgot password and save new password to computer...”* (for Tiny Web Filter Pro, [86]).
4. *“New apps don't appear in the admin panel until they've been used on the phone. A blocked app can be opened, though not used”* (for Qustodio, [101]).
5. *“My only problem is that the app stops working suddenly without notice and my kids sometimes go a few days without it , so I really have to be on top of it and make sure is sign in and working at all times”* (for Qustodio, [103]).
6. *“There is no way to limit just the internet time vs usage time. Thus, if my child needs to do offline homework on his computer, the timer starts the minute he logs into his account and will cut him off by the time he has finished and gets his internet reward”* (for Qustodio, [103]).
7. *“Kids can figure out how to take it off. I paid for a 2 year subscription and it has many good features, however, my son figured out how to take it off, so it is completely useless now and two years of money down the drain”* (for Qustodio, [103]).
8. No keyword blocks (for Qustodio, [102]).
9. No request access system (for Qustodio, [102]).
10. Reporting and notification features do not include the option to send you text alerts (for Qustodio, [104]).
11. *“I have seen my kids disabling it (clicking the right button on chrome logo shows this extension). This app works great but an intelligent kid can easily remove it. So it's actually not working for me”* (for MetaCert, [105]).
12. *“Cannot add specific web addresses. Failed to block what I needed”* (for MetaCert, [105]).
13. The extension is not blocking the adult videos on YouTube (for MetaCert, [105]).

#### What users recommend:

1. Have the ability to reset the password (for Tiny Web Filter Pro, [86])
2. To have available this google chrome extension in Android or IOS devices (for Tiny Web Filter Pro, [86]).
3. Have the control as a user (as admin) to get the notification with some way, whenever the extension being off or deleted by someone else user (for Tiny Web Filter Pro, [86]).

4. *“I wish the browser was a little more full-featured. It would be nice to be able to organize and rename/edit the bookmark names. It would also be nice if it would drop down the list of pages you have already searched in the browser”* (for Qustodio, [103]).
5. *“If there are XXX website, I would like to be able to suggest it to you as a XXX website, so it can be a collaborative stuff and more efficient blocking program”* (for MetaCert, [105]).
6. *It shouldn't be shown in the background. And it should have a 'full hide' option”* (for MetaCert, [105]).
7. Password protection (for MetaCert, [105]).

### 8.3. Eye tracking studies

For the eye trackign study we followed the following procedure:

- a) Before a participant take part in the experiment s/he was informed verbally about the study and was asked to sign a consent. The consent form aimed to make clear that answers or data collected, will be used only for research purposes without relating them to any collected demographic data.
- b) The Ex-ante questionnaire (demographics, number of children and their ages, experience with specific software, willingness of usage, expectations of such softwares) was then administered.
- c) This was followed with the eye tracking experiment / complete a task and interacting with the softwares / add-ons.
- d) After completing the experiment, they were asked to complete a questionnaire for usability evaluation of the software used in the study. This questionnaire was based on a Likert scales from 1 to 5 (where 1 means “At All” and 5 means “Great”). Parents were asked to choose which number is most representative of their opinion and their experience in the software environment. Parents were also able to express their opinions about the most useful elements of each software and point what feautres might be missing.

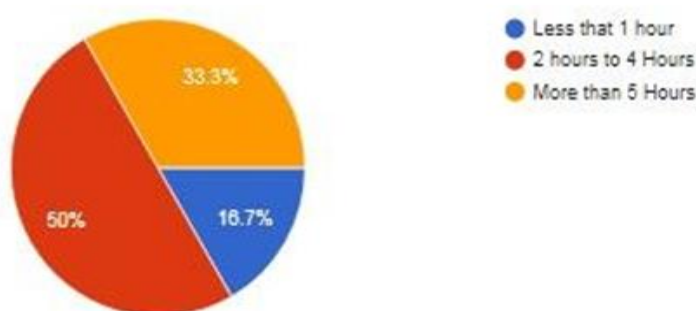
The participants were 7 Cypriot parents (6 mothers and 1 father). Our participants have children from 2 until 16 years old.

## 8.4. Results

### 8.4.1. Ex-ante questionnaire analysis results

The ex-ante questionnaire aims to identify the attitudes parents have for softwares and programs which promote web security. This questionnaire also calculates the previous experience parents had with those softwares. Finally, it tries to indicate if parents check their children’s online behaviour. From the analysis, we can see that the majority of children have access to the internet, while the majority of parents check their children’s behaviour online and they are familiar with what online content their children interact.

Some parents declared that they catch their children while they were viewing inappropriate content for their ages. The content was based on pornography and generally naked pictures, songs with abusive lyrics and risky games. Moreover, all parents didn’t have the opportunity to use any kind of program or software that offers web security on the Internet. However, all of them are willing to use them, as they believe that security on the internet is a fundamental parameter.



**Figure 50. Answers form the Quest. "If your children have access to the internet how many hours they use it per day?"**

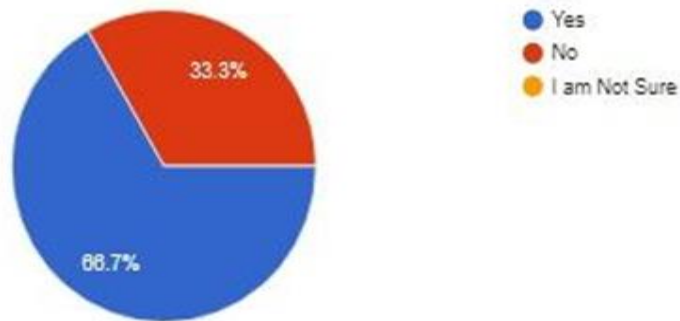


Figure 51. Answers on the Quest. "Do you check where exactly your children surf on the Internet?"

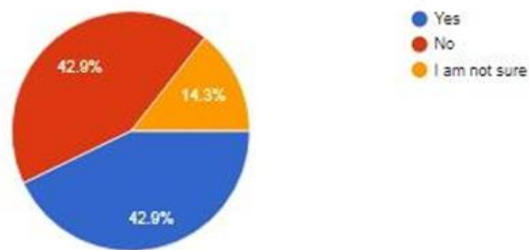


Figure 52. Answers on the Quest. “Did you see anytime, that your children were at an inappropriate for his/her age area on the internet?”

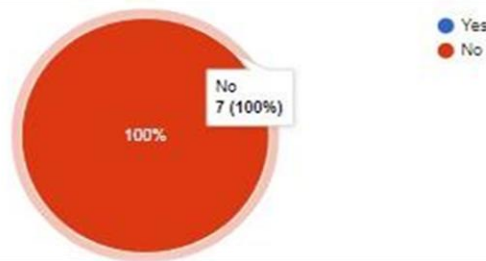


Figure 53. Answers on the Quest. “Do you use any program or software that monitors your childrens’ behaviour on the internet?”

#### 8.4.2. Software & Add-ons evaluation results

In this section we include the results of the study of the 3 security tools after the analysing the answers from the questionnaires.

**Qustodio Analysis:** Qustodio was the first software that we examined through the eye tracker system. We can see below some pictures from the use of the software using eye tracking evaluation software.



Figure 54. Installation page



Figure 55. Import children

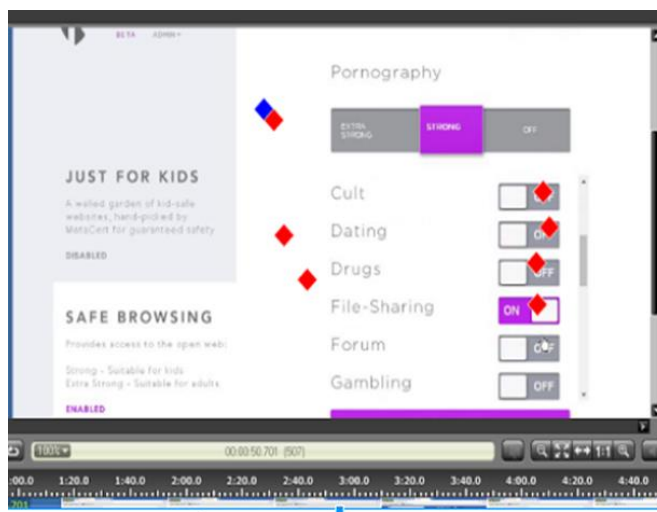


Figure 56. Choose categories of content to be blocked

**MetaCert Analysis:** MetaCert was the second software that we investigated. Bellow you can see pictures from the eye tracking software while parents were using it.

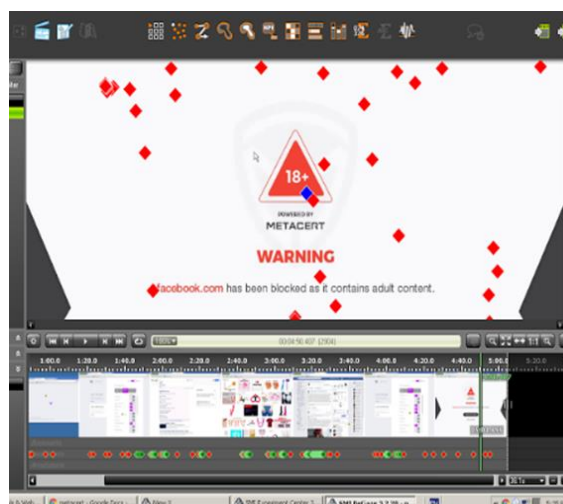


Figure 57. Notification that website is blocked (Facebook)



## 9. Discussion / Conclusion

This deliverable reports on six studies carried out to investigate the user and societal aspects of security and privacy of OSNs.

This was achieved through three review based studies and three experimental studies that looked at:

(a) User behavior and experience when faced with security and privacy risks on OSN (study 1). The literature in study 1 helped us document the types of concerns and behaviors users have when faced with security and privacy risks online and on OSNs more specifically

(b) Cyberbullying (study 2). This study helped us document the different user profiles that appear in OSNs during cyberbullying activity.

(c) E-safety in Web 2.0 Learning Environments (study 3) which helped us identify the security and privacy challenges when using web2.0 services for learning.

(d) a study discovering social bridges in Microblogs (study 4) which helped us to demonstrate how Social Network Analysis can reveal useful information regarding OSN security and privacy. A new category of influential Twitter users is identified and associated with malicious behavior across the Twitter user graph. The different behavioral patterns of these two categories of users that pose dangers to particularly vulnerable groups of users (such as children) and their intrinsic characteristics are explored to allow for alerts to occur when a new connection is added. In the future, we plan to expand the features used to include semantic or textual information and apply our best performing classification scheme to other OSNs, as well.

(e) an extensive survey of use of OSNs by minors (study 5) in three different countries (Greece, UK, Cyprus) revealing individual and cultural differences in terms of security and privacy in OSNs

(f) a usability evaluation of fraud detection systems (study 6) revealing limitations and prospective design considerations regarding OSN privacy and security detection software.

The results of these studies and task (T3.1), in combination with the upcoming tasks (T3.2, T3.3) will lead to the development of design guidelines for the design of OSN privacy and security detection software systems (T3.4).



## 10. Appendices

### 10.1. Appendix 1: The Questionnaire used in the study

This questionnaire created for research purposes of ENCASE project (Enhancing security and privacy in the Social web | *More at the website: [encase.socialcomputing.eu](http://encase.socialcomputing.eu)*). This questionnaire aimed mainly at students aged between 12 to 17 who hold personal account/s in social networks. It is asserted that the participation is anonymous and confidentiality of the participants' data items will be strictly maintained.

---

Gender:

- Male
- Female

**City of residence:**  Milton Keynes  Other \_\_\_\_\_

Age: \_\_\_\_

Educational level:

- Middle School
- High-School
- Higher Education
- Don't answer

Part A

1. In general, how concerned are you about security on the Internet? (e.g people reading your email, finding out what websites you visit, etc.)

- Not at all concerned
- A little concerned
- Somewhat concerned
- Very concerned
- I know I should be concerned, but I'm not

2. Are you willing to use your credit card on the web?

- Yes
- No

Don't answer

3. Do you buy online?

Yes

No

Don't answer

4. Do you think rating on how "secure" is one specific website is it helpful or have any value to you?

Yes

No

Don't answer

5. While using the internet, have you ever done any of the following things? Have you ever [insert items - a, b & c] while you used the internet: (circle your answer)

**a.** used a temporary username or email address?

Yes / No / Don't answer / Don't know

**b.** used a fake name or untraceable username?

Yes / No / Don't answer / Don't know

**c.** given inaccurate or misleading information about yourself?

Yes / No / Don't answer / Don't know

## Part B

1. Are you a member of any online social network?

Yes

No

2. How many social networking sites/communities are you a member of?

- None
- 1 - 4
- 4 - 8
- More

3. I joined for the first time a social network at age of \_\_\_\_\_.

4. Usually, how do you access your social network account? (You can choose more than one)

- PC / Laptop
- Smartphone
- Tablet
- Other (please specify): \_\_\_\_\_

5. On average, how much time do you spend daily on social networking sites?

- Less than 1 hour
- 1 - 2 hrs per day
- 3 - 4 hrs per day
- 4 - 6 hrs per day
- 6+ more hrs per day

6. How many contacts/friends do you have in total in all of your social networks sites? (Select with a v)

Fewer than 150	150-300	301-600	601-900	901-1500	1500-2500	More than 2500+

7. About how many of your friends on your social networks sites do you consider that you know them?

- All of them
- Most of them
- About half of them
- A few of them

8. Do you accept friend requests / or follow request from strangers who are on social network sites?

- Yes
- Sometimes
- No

9. Have you ever met with somebody (you didn't know personally before) after chatting through a social network site?

- Yes
- No
- Don't answer

10. Would you trust random strangers to view your profile?

- Yes
- No
- Don't answer

11. Do you trust all your connected friends with all parts of your profile?

- Yes, all these friends
- Some of these friends
- No
- Don't care

12. Are you "connected" with stranger "friends" from abroad on your social network accounts?

- Yes
- No

13. Do you ever worry about how much information is available about you on the internet, or is that not something you worry about?

- Yes, worry about it
- No, don't worry about it
- Don't know

14. How concerned are you about your security and privacy of your sensitive content (personal information) on your social networks?

- Not at all concerned
- A little concerned
- Somewhat concerned
- Very concerned
- I know I should be concerned, but I'm not

15. Are you interested in controlling the privacy settings of your account?

- Yes
- No
- I don't know

16. Have you changed the privacy settings of your account/s?

- Yes
- No
- I don't know

17. How do you control the privacy settings of your social media accounts? Select the most valid for you

- I adjust my privacy settings to control who has access to what I publish on my account
- I am aware of different levels of privacy but don't really care about controlling them
- I am not sure how I can control the privacy settings on my social media accounts
- Other (please specify): \_\_\_\_\_

18. What device do you use to change the privacy settings?

- My mobile phone
- PC / laptop
- PC / Laptop and Mobile phone
- Other (please specify): \_\_\_\_\_

19. Please indicate if now online you provide the following information for yourself in one of your social accounts (If Yes please select in which privacy settings provided) (Note with √ / x)

	YES	YES	YES	
Personal Details:	In public view	In friends/followers view	With “only me” view (locked)	NO

Real Name				
Real Surname				
A photo of you				
Photos of your friends				
Your cell number				
Which groups/orgs you belong to				
Friends list / Followers list				
Things you’ve written using your name				
Your employer/company you work for				
Your school/university you study/studied				
Your relationship status				
Your email address				
The date of your birthday				
Your birth year				
Video of you				

Your political views				
Nationality				
Religion				
Links to other social accounts of you				

20. From the elements of Q.19 page 5 (left column), please note at least 1 (to 3) personal details, which you perceive them as important sensitive content for yourself.

1. \_\_\_\_\_
2. (optional) \_\_\_\_\_
3. (optional) \_\_\_\_\_

21. Do you think controlling access to certain content on your profile is necessary for your accounts on online social networks?

- Yes
- No
- Don't care

22. Do you think you can recognize a fake account?

- Yes
- Sometimes
- No
- Don't answer

23. Have you ever provide fake personal details:

	Yes	No
a) to create a personal account in social network site?		
b) during chatting through social network site?		
c) when you answer questions from strangers?		

24. Please note the if you agree or not with the following statements: Please choose with √ from a

scale of 1 to 5

1: Strongly Disagree / 2: Disagree / 3: Maybe / 4: Agree / 5: Strongly agree

	1	2	3	4	5
I understand that there are dangerous people in social network sites					
I don't believe that there are dangers if the stranger "friend" lives abroad					
The nationality of the stranger "friend" affects me to what way I can interact with him/her					
During chatting in social network site If a local "friend" asked me to provide some personal details, maybe I would do it.					
During chatting in social network site If a "friend" from abroad asked me to provide some personal details, maybe I would do it.					

25. During your experience in social networks have you ever found yourself to be faced with a cyber bullying?

- Yes
- No
- Don't answer

26. During your experience in social networks have you ever found yourself to be faced with the threat sexual abuse in your private life?

- Yes
- No
- Don't answer

27. Have you ever "fight" with somebody another user on your social network account? (e.g. during chatting, or in comments on a post)

- Yes
- No
- Don't answer

28. Through your experience on social networks have you ever feel that you are in danger in some way?

- Yes
- No

Part C



1. Are you satisfied with current privacy controls methods?

- Yes
- No
- Don't care

2. Would you prefer more advanced settings to protect your privacy on online social networks?

- Yes
- No
- I don't know

3. Would you be eager to provide individual characteristics to protect your personal data online?

- Yes
- Maybe
- No
- I don't know

4. If a new tool applied to your social networks accounts with a goal of an implicit protection of your sensitive content information, how acceptable are you to provide to the system characteristics such as:

Please choose with √ from a scale of 1 to 5

1: Strongly Disagree / 2: Disagree / 3: Maybe / 4: Agree / 5: Strongly agree

	1	2	3	4	5
a) your face scan?					
b) your finger prints?					

5. Do you think you would feel more protected if you provide these characteristics?

- Yes
- Maybe
- No
- I don't know

Follow-up Questionnaires: Would you be interested in taking part in follow-up questionnaires of the research in the future?



Deliverable D3.1 “Report on user and societal aspects, and on usability of security and privacy OSN systems”

Yes, why not    No sorry

If you have chosen “Yes” in the above question, please tell us your email address:

Email: \_\_\_\_\_

Thank you very much for your participation and your time!

## 11. References

1. ENCISE: ENhancing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors. (2015). MENA Report, n/a.
2. Harte, R., Glynn, L., Rodríguez-Molinero, A., Baker, P., Scharf, T., Quinlan, L. and ÓLaighin, G. (2017). A Human-Centered Design Methodology to Enhance the Usability, Human Factors, and User Experience of Connected Health Systems: A Three-Phase Methodology. <http://humanfactors.jmir.org/2017/1/e8/>
3. J. Wang and S. Senecal, “MEASURING PERCEIVED WEBSITE USABILITY,” *Journal of Internet Commerce*, vol. 6, no. 4, pp. 97–112, 2008.
4. D. Robins and J. Holmes, “Aesthetics and credibility in web site design,” *Information Processing & Management*, vol. 44, no. 1, pp. 386–399, Jan. 2008.
5. Sukinah Aziz, N. (2013). ASSESSING WEB SITE USABILITY MEASUREMENT. *International Journal of Research in Engineering and Technology*, [online] 02(09), pp.386-392. Available at: <https://goo.gl/U1behX>
6. Leventhal, L. and Barnes, J. (2008). Usability engineering: process, products, and examples. *Choice Reviews Online*, 45(07), pp.45-3835-45-3835.
7. Nielsen, J. 2012. Nilsen & Norman Group: Usability 101: Introduction to Usability. 4.1.2012. <http://www.nngroup.com/articles/usability-101-introduction-to-usability>.
8. The Interaction Design Foundation. (2017). *Usability Evaluation*. [online] Available at: <https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/usability-evaluation>.
9. McGrath, L. (2011). *What are the Web Content Accessibility Guidelines?*. [online] Wuhcag. Available at: <http://www.wuhcag.com/web-content-accessibility-guidelines/>.
10. Horton, S. 2006. *Universal Usability: A Universal approach to web usability*. [online] Available at: <http://universalusability.com/>.
11. Norman DA, Draper SW, editors. *User Centered System Design: New Perspectives on Human-Computer Interaction*. Hillsdale, NJ: Lawrence Erlbaum Associates; 1986.
12. Silva, C. S., Barbosa, G. A., Silva, I. S., Silva, T. S., Mourão, F., & Coutinho, F. (2017, June). Privacy for Children and Teenagers on Social Networks from a Usability Perspective: A Case Study on Facebook. In *Proceedings of the 2017 ACM on Web Science Conference* (pp. 63-71). ACM.
13. Gupta, A. and Dhami, A. (2015). Measuring the impact of security, trust and privacy in information sharing: A study on social networking sites. *Journal of Direct, Data and Digital Marketing Practice*, [online] 17(1), pp.43-53. Available at: <https://link.springer.com/article/10.1057/dddmp.2015.32>
14. Liu, Y., Gummadi, K., Krishnamurthy, B. and Mislove, A. (2011). Analyzing facebook privacy settings. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference - IMC '11*. [online] Available at: [https://www.researchgate.net/publication/238041960\\_Analyzing\\_Facebook\\_privacy\\_settings\\_User\\_expectations\\_vs\\_reality](https://www.researchgate.net/publication/238041960_Analyzing_Facebook_privacy_settings_User_expectations_vs_reality)
15. Fire, M., Goldschmidt, R. and Elovici, Y. (2014). Online Social Networks: Threats and Solutions. *IEEE Communications Surveys & Tutorials*, 16(4), pp.2019-2036.

16. Rainie, L., Kiesler, S., Kang, R. and Madden, M. (2013). *Anonymity, Privacy, and Security Online*. [online] Pew Research Center: Internet, Science & Tech. Available at: <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
17. Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. and Beaton, M. (2013). *Teens, Social Media, and Privacy*. [online] Pew Research Center: Internet, Science & Tech. Available at: <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>
18. David Hiatt and Young B. Choi, "Role of Security in Social Networking" *International Journal of Advanced Computer Science and Applications(Ijacs)*, 7(2), 2016. <http://dx.doi.org/10.14569/IJACSA.2016.070202>
19. Livingstone, Sonia and Ólafsson, Kjartan and Staksrud, Elisabeth (2011) *Social networking, age and privacy*. EU Kids Online, London, UK. Available online at: <http://eprints.lse.ac.uk/35849/>
20. Dehue F., Bolman C., and Völlink T. (2008). "Cyber-bullying: Youngsters' Experiences and Parental Perception" *CyberPsychology & Behavior*. April 2008, Vol. 11, No. 2, pp. 217-223. DOI: <https://doi.org/10.1089/cpb.2007.0008>
21. Yao M.-Z., Rice R.-E., Wallis K. (2007). "Predicting User Concerns About Online Privacy", *Journal of the American Society for Information Science and Technology*, Vol. 58, No.5, pp. 611-762. DOI: 10.1002/asi.20530
22. Dong C., Jin H., Knijnenburg B.-P. (2015). "Predicting Privacy Behavior on Online Social Networks". *AAAI Conference on Weblogs and Social Media (ICWSM)*. Retrieved June 2017 from <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/view/10554>
23. Fire M., Goldschmidt R., Elovici Y. (2014). "Online Social Networks: Threats and Solutions", *IEEE Communication Surveys & Tutorials*, Vol. 16, No. 4, Fourth Quarter 2014, pp. 2019-2036
24. Tsirtsis A., Tsapatsoulis N., Stamatelatos M., Papadamou K., Sirivianos M. (2016). "Cyber Security Risks for Minors: A Taxonomy and a Software Architecture". In *2016 11th International Workshop on Semantic and Social Media Adaptation and Personalization (SMAP)*. Thessaloniki, Oct. 20-21, 2016, IEEE. DOI: <https://doi.org/10.1109/SMAP.2016.7753391>
25. Jang-Jaccard J. & Nepal S. (2014). "A survey of emerging threats in cybersecurity". *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp. 973–993. DOI: <http://dx.doi.org/10.1016/j.jcss.2014.02.005>.
26. Jin T., Chen Y., Wang T., Pan H., Vasilakos A.-V. (2013). "Understanding User Behavior in Online Social Networks: A Survey". *IEEE Communication Magazine*, Vol. 51, No. 9, pp. 144-150. DOI: <https://doi.org/10.1109/MCOM.2013.6588663>
27. McGrath F. (2017). "Top 10 Reasons for Using Social Media", *GlobalWebIndex*, June 7, 2017. Retrieved August 2017 from: <http://blog.globalwebindex.net/chart-of-the-day/social-media/>
28. Gangadharbatla H. (2008). "Facebook Me: Collective Self-Esteem, Need to Belong, and Internet Self-Efficacy as Predictors of the iGeneration's Attitudes toward Social Networking Sites". *Journal of Interactive Advertising*, Vol. 8, No. 2. DOI: 10.1080/15252019.2008.10722138
29. Kisekka V., Bagchi-Sen S., Raghav Rao H. (2013). "Extent of private information disclosure on online social networks: An exploration of Facebook mobile phone users". *Computers in Human Behavior*, Vol. 29, (2013), pp. 2722–2729. DOI: <https://doi.org/10.1016/j.chb.2013.07.023>
30. 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". *Online*

- Journal of Applied Knowledge Management*, Vol. 3, No. 1, pp. 108-207. Retrieved June 2017 from [http://www.iiakm.org/ojakm/articles/2015/volume3\\_1/OJAKM\\_Volume3\\_1pp180-207.pdf](http://www.iiakm.org/ojakm/articles/2015/volume3_1/OJAKM_Volume3_1pp180-207.pdf)
31. Sundar S.-S. & Marathe S.-S. (2010). “Personalization versus customization: The importance of agency, privacy, and power usage”. *Human Communication Research*, Vol. 36, No. 3, pp. 298–322. DOI: <http://dx.doi.org/10.1111/j.1468-2958.2010.01377.x>.
  32. Fogel J. & Nehmad E. (2009). “Internet social networking communities: Risk taking, trust, and privacy concerns”. *Computers in Human Behavior*, Vol. 25, No. 1, pp. 153-160. DOI: <https://doi.org/10.1016/j.chb.2008.08.006>
  33. Canadian Centre for Child Protection. (July 26, 2017). “Statement: new statistics Canada Report reflects alarming reality of sexual abuse of children”. Retrieved August 12, 2017 from: [https://www.protectchildren.ca/app/en/media\\_release\\_201707\\_statcan\\_report\\_child\\_sexual\\_abuse](https://www.protectchildren.ca/app/en/media_release_201707_statcan_report_child_sexual_abuse)
  34. Kidshealth. (2017). “Cyber-bullying”. Retrieved July 2017 from <http://kidshealth.org/en/parents/cyber-bullying.html>
  35. Hugi U. (2011). “Reviewing person's value of privacy of online social networking”. *Internet Research*, Vol. 21, No. 4, pp. 384-407. DOI: <http://dx.doi.org/10.1108/10662241111158290>
  36. Madejski M., Johnson M., Bellovin S.-M. (2011). “The Failure of Online Social Network Privacy Settings”. *Columbia University Academic Commons*, DOI: <https://doi.org/10.7916/D8NG4ZJ1>
  37. Li Y., Li Y., Yan Q., Deng R.-H. (2015). “Privacy leakage analysis in online social networks”. *Computers & Security*, Vol. 49, pp. 239-254. DOI: <https://doi.org/10.1016/j.cose.2014.10.012>
  38. Patsakis C., Zigomitos A., Papageorgiou A., Solanas A. (2014). “Privacy and Security for Multimedia Content shared on OSN: Issues and Countermeasures”, *Computer Journal*, Vol. 58, No. 4, pp. 518-535. DOI: <https://doi.org/10.1093/comjnl/bxu066>
  39. Angulo J. & Ortlieb M. (2015). “WTH..!?!” Experiences, reactions, and expectations related to online privacy panic situations”. In *Proceedings of the Symposium on Usable Privacy and Security (SOUP)*. Ottawa, Canada, July. 22-24, 2015. Retrieved August 12, 2017 from: <https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo>
  40. Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. *Journal of child psychology and psychiatry*, 49(4), 376-385.
  41. Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., & Menesini, E. (2010). Cyberbullying: Labels, behaviours and definition in three European countries. *Australian Journal of Guidance and Counselling*, 20(02), 129-142.
  42. Smith-Ross, C., Esmail, A., Omar, A., & Franklin, K. (2014). Chapter Nine Bullying: Recognizing the Warning Signs. *Alleviating bullying: Conquering the challenge of violent crimes*, 146.
  43. Foody, M., Samara, M., & Carlbring, P. (2015). A review of cyberbullying and suggestions for online psychological therapy. *Internet Interventions*, 2(3), 235-242.
  44. Schneider, S. K., O'Donnell, L., Stueve, A., & Coulter, R. W. (2012). Cyberbullying, school bullying, and psychological distress: A regional census of high school students. *American Journal of Public Health*, 102(1), 171-177.
  45. Al Mazari, A. (2013). Cyber-bullying taxonomies: Definition, forms, consequences and mitigation strategies. 5th International Conference on Computer Science and Information Technology

- (CSIT) (pp. 126- 133). IEEE.
46. Kyriacou, C., & Zuin, A. (2016). Cyberbullying and moral disengagement: an analysis based on a social pedagogy of pastoral care in schools. *Pastoral Care in Education*, 34(1), 34-42.
  47. You, S., & Lim, S. A. (2016). Longitudinal predictors of cyberbullying perpetration: Evidence from Korean middle school students. *Personality and Individual Differences*, 89, 172-176.
  48. Sourander, A., Klomek, A. B., Ikonen, M., Lindroos, J., Luntamo, T., Koskelainen, M., . . . Helenius, H. (2010). Psychosocial risk factors associated with cyberbullying among adolescents: A population-based study. *Archives of general psychiatry*, 67(7), 720-728.
  49. Barlinska, J., Szuster, A., & Winiewski, M. (2013). Cyberbullying among adolescent bystanders: Role of the communication medium, form of violence, and empathy. *Journal of Community & Applied Social Psychology*, 23(1), 37-51.
  50. Sanchez, F. C., Romero, M. F., Navarro-Zaragoza, J., Ruiz-Cabello, A. L., Frantzisko, O. R., & Maldonado, A. L. (2016). Prevalence and patterns of traditional bullying victimization and cyber-teasing among college population in Spain. *BMC public health*, 16(1), 1.
  51. Li, Q. (2006). Cyberbullying in schools a research of gender differences. *School psychology international*, 27(2), 157-170.
  52. Lapidot-Lefler, N., & Dolev-Cohen, M. (2015). Comparing cyberbullying and school bullying among school students: prevalence, gender, and grade level differences. *Social psychology of education*, 18(1), 1-16.
  53. Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard a preliminary look at cyberbullying. *Youth violence and juvenile justice*, 4(2), 148-169.
  54. Keith, S., & Martin, M. E. (2005). Cyber-bullying: Creating a culture of respect in a cyber world. *Reclaiming children and youth*, 13(4), 224.
  55. Kowalski, R. M., & Limber, S. P. (2007). Electronic bullying among middle school students. *Journal of adolescent health*, 41(6), S22--S30.
  56. Mishna, F., Khoury-Kassabri, M., Gadalla, T., & Daciuk, J. (2012). Risk factors for involvement in cyber bullying: Victims, bullies and bully--victims. *Children and Youth Services Review*, 34(1), 63-70.
  57. Pabian, S., & Vandebosch, H. (2016). An investigation of short-term longitudinal associations between social anxiety and victimization and perpetration of traditional bullying and cyberbullying. *Journal of youth and adolescence*, 45(2), 328-339.
  58. Steffgen, G., Konig, A., Pfetsch, J., & Melzer, A. (2011). Are cyberbullies less empathic? Adolescents' cyberbullying behavior and empathic responsiveness. *Cyberpsychology, Behavior, and Social Networking*, 14(11), 643-648.
  59. Tangen, D., & Campbell, M. (2010). Cyberbullying Prevention: One Primary School's Approach. *Australian Journal of Guidance and Counselling*, 20(02), 225-234
  60. Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of adolescent health*, 41(6), S51--S58.
  61. Sengupta, A., & Chaudhuri, A. (2011). Are social networking sites a source of online harassment for teens? Evidence from survey data. *Children and Youth Services Review*, 33(2), 284-290.
  62. Corcoran, L., Guckin, C. M., & Prentice, G. (2015). Cyberbullying or cyber aggression?: A review

- of existing definitions of cyber-based peer-to-peer aggression. *Societies*, 5(2), 245-255.
63. Hosseinmardi, H., Mattson, S. A., Rafiq, R. I., Han, R., Lv, Q., & Mishra, S. (2015). Detection of cyberbullying incidents on the instagram social network. arXiv preprint arXiv:1503.03909.
  64. Vandebosch, H., & Van Cleemput, K. (2009). Cyberbullying among youngsters: Profiles of bullies and victims. *New media & society*, 11(8), 1349-1371.
  65. Langos, C. (2012). Cyberbullying: The challenge to define. *Cyberpsychology, Behavior, and Social Networking*, 15(6), 285-289.
  66. Pieschl, S., Porsch, T., Kahl, T., & Klockenbusch, R. (2013). Relevant dimensions of cyberbullying—Results from two experimental studies. *Journal of Applied Developmental Psychology*, 34(5), 241-252.
  67. Sticca, F., & Perren, S. (2013). Is cyberbullying worse than traditional bullying? Examining the differential roles of medium, publicity, and anonymity for the perceived severity of bullying. *Journal of youth and adolescence*, 42(5), 739-750.
  68. Potha, N., & Maragoudakis, M. (2014). Cyberbullying detection using time series modeling. 2014 IEEE International Conference on Data Mining Workshop, (pp. 373-382).
  69. Slonje, R., Smith, P. K., & Frisen, A. (2013). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior*, 29(1), 26-32.
  70. Englander, E. (2012). Spinning our wheels: Improving our ability to respond to bullying and cyberbullying. *Child & Adolescent Psychiatric Clinics of North America*.
  71. Ioannou, A., Blackburn J., Stringhini, G., De Cristofaro, E., Kourtellis N., Sirivianos, M., Zaphiris, P. (2017). From Risk Factors to Detection and Intervention: A Metareview and Practical Proposal for Research on Cyberbullying, in *IST-Africa 2017*
  72. Yin , D., Xue, Z., Hong , L., Davison, B., Kontostathis, A., & Edwards, L. (2009). Detection of harassment on web 2.0., (p. in *Proceedings WWW’2009 Workshop on Content Analysis in the WEB 2.0 (CAW2.0)*). Madrid, Spain.
  73. Yip, M., Shadbolt, N., & Webber, C. (2012). Structural analysis of online criminal social networks. *in Proceedings IEEE Conference on Intelligence & Security Informatics (ISI)*, (pp. pp. 60–65). ,Washington, DC.
  74. Grier, C., Thomas, K., Paxson, V., & Zhang, M. (2010). @spam: The underground on 140 characters or less. *in Proceedings 17th ACM Conference on Computer & Communications Security (CCS)*, (pp. pp. 27–37). Chicago, IL.
  75. R. Heartfield and G. Loukas. (2015). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, vol. 48, no. 3, pp. 37:1–37:39.
  76. Thomas, K., Grier, C., Song, D., & Paxson, V. (2011). Suspended accounts in retrospect: An analysis of twitter spam. *in Proceedings ACM SIGCOMM Conference on Internet Measurement Conference (IMC)*, (pp. pp. 243–258). Tokyo Japan.
  77. Yang, C., Harkreader, R., Zhang, J., Shin, S., & Gu, G. (2012). Analyzing spammers’ social networks for fun and profit: A case study of cyber criminal ecosystem on twitter. *in Proceedings 21st International Conference on World Wide Web (WWW)*. Lyon, France.
  78. Ghosh, S., Viswanath, F., Sharma, N., & Korlam, G. (2012). Understanding and combating link farming in the twitter social network. *in Proceedings 21st International Conference on World Wide Web (WWW)*. Lyon, France.

79. Tarjan, R. (1972). Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, vol. 1, no. 2, pp. 146–160.
80. Estrada, E. (2012). *The Structure of Complex Networks: Theory and Applications*. Oxford University Press.
81. Parmaxi, A., Papadamou, K., Sirivianos, M., & Stamatelatos, M. (2017, July). E-safety in Web 2.0 Learning Environments: A Research Synthesis and Implications for Researchers and Practitioners. In *International Conference on Learning and Collaboration Technologies* (pp. 249-261). Springer, Cham.
82. ENCASE: EnhaNcing seCurity And privacy in the Social wEb: a user centered approach for the protection of minors. (2016). Deliverable D2.2 “System Requirements and Software Architecture”.
83. Protect, understand and manage your kids’ internet activity with Qustodio. <https://www.qustodio.com/en/>
84. Computer & Mobile monitoring software. <http://www.webwatcher.com/?refID=Inkshr&siteID=Cty0dj6o3sg-GHtU.M9eT5Zlm7qQ5Ms1ig>
85. PureSight Online child safety. <http://puresight.com/puresight-prevents-cyberbullying.html>
86. TinyFilter PRO - the best Web Filter addon <https://chrome.google.com/webstore/detail/tinyfilter-pro-the-best-w/jchoeoanokglloibgmlombfgpdoaido>
87. The Parental control for Firefox. <https://addons.mozilla.org/en-US/firefox/addon/foxfilter/>
88. MetaCert Security API. <https://metacert.com/>
89. eSafely protects you where your Web filter doesn’t. <http://www.esafely.com/>
90. Aldhafferi, N., Watson, C. and A.S.M, S. (2013). Personal Information Privacy Settings of Online Social Networks and Their Suitability for Mobile Internet Devices. *International Journal of Security, Privacy and Trust Management*, 2(2), pp.1-17.
91. Anon, (1998). *Online Privacy and Security Questionnaire*. [online] Available at: [https://www.cc.gatech.edu/gvu/user\\_surveys/survey-1998-10/questions/privacy.html](https://www.cc.gatech.edu/gvu/user_surveys/survey-1998-10/questions/privacy.html)
92. Chieng, L., Singh, M., Zaaba, Z. and Hassan, R. (2015). Multi-Facet Trust Model for Online Social Network Environment. *International Journal of Network Security & Its Applications*, 7(1), pp.1-18.
93. Koehorst, R. (2013). *Personal Information Disclosure on Online Social Networks*. [online] Essay.utwente.nl. Available at: [http://essay.utwente.nl/63797/1/MSc\\_Ruud\\_H.G\\_Koehorst.pdf](http://essay.utwente.nl/63797/1/MSc_Ruud_H.G_Koehorst.pdf)
94. Lenhart, A. and Madden, M. (2007). *Teens, Privacy and Online Social Networks*. [online] Pew Research Center: Internet, Science & Tech. Available at: <http://www.pewinternet.org/2007/04/18/teens-privacy-and-online-social-networks/>
95. Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. and Beaton, M. (2013). *Teens, Social Media, and Privacy*. [online] Pew Research Center: Internet, Science & Tech. Available at: <http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/>
96. Marketest.co.uk. (2017). *Social Networking Websites Questionnaire - Market Research Survey*. [online] Available at: <http://www.marketest.co.uk/market-research-questionnaire/47/social-network-websites>



97. My3q.com. (2017). *Survey Summary - A Survey about Privacy Settings in an Online Social Network - Facebook*. [online] Available at: <http://www.my3q.com/research/comm7030gp2/52625.phtml>
98. Rainie, L., Kiesler, S., Kang, R. and Madden, M. (2013). *Anonymity, Privacy, and Security Online*. [online] Pew Research Center: Internet, Science & Tech. Available at: <http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/>
99. Surveymonkey.com. (2017). *Online Social Networking Questionnaire Survey*. [online] Available at: <https://www.surveymonkey.com/r/LMWLMLS>
100. Surveymonkey.com. (2017). *Social Media Privacy Survey*. [online] Available at: <https://www.surveymonkey.com/r/socialmediaprivacy>
101. Hall B. (2017). *Qustodio for Families Premium Review*. [online] Tom's Guide. Available at: <https://www.tomsguide.com/us/qustodio-for-families,review-2752.html>
102. Stobing C. (2016). *Qustodio Review 2017, Is this Parental Control any good? | Comparitech*. [online] Comparitech. Available at: <https://www.comparitech.com/parental-control/reviews/qustodio-review/>
103. Amazon.com. (2017). *Amazon.com: Customer reviews: Qustodio Parental Control*. [online] Available at: [https://www.amazon.com/Qustodio-Parental-Control/product-reviews/B00CM7FLSK/ref=cm\\_cr\\_getr\\_d\\_show\\_all?pageNumber=1&reviewerType=all\\_reviews](https://www.amazon.com/Qustodio-Parental-Control/product-reviews/B00CM7FLSK/ref=cm_cr_getr_d_show_all?pageNumber=1&reviewerType=all_reviews)
104. Shipley, R. (2017). *Qustodio Premium 5 Review - Pros, Cons and Verdict*. [online] TopTenReviews. Available at: <http://www.toptenreviews.com/software/security/best-internet-filter-software/qustodio-review/>
105. Chrome.google.com. (2017). *Parental Controls & Web Filter from MetaCert*. [online] Available at: <https://chrome.google.com/webstore/detail/parental-controls-web-fil/dpfbddcgbimoafpgmbbjliegkfcjkmn/support>
106. Gogoglou, A., Theodosiou, Z., Kounoudes, T., Vakali, A., & Manolopoulos, Y. (2016, December). *Early malicious activity discovery in microblogs by social bridges detection*. In *Signal Processing and Information Technology (ISSPIT), 2016 IEEE International Symposium on* (pp. 132-137). IEEE.