future internet

MDPI

Article

Privacy and Security Issues in Online Social Networks

Shaukat Ali [1,*], Naveed Islam [1], Azhar Rauf [2], Ikram Ud Din [3] and Mohsen Guizani [4] and Joel J. P. C. Rodrigues [5,6,7]

1 Department of Computer Science, Islamia College University, Peshawar 25120, Pakistan; naveed.islam@icp.edu.pk
2 Department of Computer Science, University of Peshawar, Peshawar 25120, Pakistan; azhar.rauf@uop.edu.pk
3 Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan; ikramuddin205@yahoo.com
4 Computer Science and Engineering Department, Qatar University, Doha 2713, Qatar; mguizani@ieee.org
5 Post-graduation, National Institute of Telecommunications (Inatel), 37540-000 Santa Rita do Sapucaí-MG, Brazil; joeljr@ieee.org
6 Covilhã Delegation, Instituto de Telecomunicações, 1049-001 Lisbon, Portugal
7 PPGIA, University of Fortaleza (UNIFOR), 90811-905 Fortaleza-CE, Brazil
* Correspondence: shaukat@icp.edu.pk

Received: 29 September 2018; Accepted: 21 November 2018; Published: 22 November 2018

Abstract: The advent of online social networks (OSN) has transformed a common passive reader into a content contributor. It has allowed users to share information and exchange opinions, and also express themselves in online virtual communities to interact with other users of similar interests. However, OSN have turned the social sphere of users into the commercial sphere. This should create a privacy and security issue for OSN users. OSN service providers collect the private and sensitive data of their customers that can be misused by data collectors, third parties, or by unauthorized users. In this paper, common security and privacy issues are explained along with recommendations to OSN users to protect themselves from these issues whenever they use social media.

Keywords: OSN; security; classic privacy threats; modern threats

1. Introduction

Social media are a source of communication between the data owner (data generator) and viewers (end users) for online communications that create virtual communities using online social networks (OSN) [1]. A social network is a social graph that represents a relationship among users, organizations, and their social activities. These users, organizations, groups, etc., are the nodes, and the relationships between the users, organizations, groups are the edges of the graph. An OSN is an online platform used by end users to create social networks or relationships with other people that have similar views, interests, activities, and/or real-life connections [2]. A large number of different types of social-networking services are available in the current online space. The following are some of the common features in social-networking sites [2,3]:

- All current online social-networking services are web-based, using an Internet connection. Contents are stored on cloud storage through a centralized access management system. These contents can be accessed from anywhere using an Internet connection and web browsers.
- OSN users need to create a public profile for social-network sites as per their predefined format. This profile information is primarily used for the authentication process to log into the social-networking site.

- Almost all existing social-networking services facilitate users in developing their social relations with other users by connecting a user's profile with others having similar profile information.
- One interesting feature of the existing OSNs is that contents on these sites are user-generated, while OSNs use these contents for business purposes.

The main goal of OSNs is to share contents with maximum users. Users utilize OSNs, such as Facebook, Twitter, and LinkedIn, to publish their routine activities. Sometimes, OSN users share information about themselves and their lives with friends and colleagues. However, in these published data, some of the revealed contents through the OSN are private and therefore should not be published at all. Typically, users share some parts of their daily life routine through status updates or the sharing of photographs and videos. Currently, various OSN users utilize smartphones to take pictures and make videos for sharing through OSNs. These data can have location information and some metadata embedded in it. OSN service providers collect a range of data about their users to offer personalized services, but it could be used for commercial purposes. In addition, users' data may also be provided to third parties, which lead to privacy leakages. This information can allow malicious users to leverage and invade the privacy of an individual [4]. Information retrieval and data privacy are two growing areas in computer-science disciplines that have different goals. Information retrieval provides methods for data extraction. It also offers a set of techniques to an organization for data analysis and making decisions based on this retrieved information. Data privacy protects information from unauthorized and malicious access that discloses, modifies, attacks, or destroys the data stored or shared online. For example, researchers related to information retrieval sometimes do not consider privacy issues while designing solutions for information retrieval and management. On the other hand, researchers who work on data privacy usually restrict information-retrieval techniques to protect sensitive data from adversaries who seek personal information.

With the emergence of social media and the growing popularity of online communication using OSNs, more sensitive information about individuals is available online. Though much of the data that are shared through OSNs are not sensitive, some users publish their personal information. Thus, the availability of publicly accessible sensitive data can lead to the disclosure of user privacy. The privacy of users is at more risk when publicly available data can be traced, and their activities can be connected with these data for mining and extracting sensitive information from it.

Privacy has different meanings in different situations, and the intensity of privacy depends upon the context of shared contents. Nissenbaum [5] explained the ultimate value of the data be protected in order to safeguard the contextual integrity of the online shared data. Information gathered from social media for analysis purposes is generally unintended and often irrelevant. However, it may be related to the private activities of a person, for example, religion or political affiliations [6].

The main focus of the paper is to point out that privacy and security issues related to OSN, and educate ordinary users on how to protect themselves from these security and privacy issues. Privacy is the right of someone to keep information to themselves or at least share it only with relevant people. Privacy-preservation and -protection terms are used to keep private information away from irrelevant users. The term 'privacy preservation' is used in situations when private data are handed over to some other party, an OSN in this case, and the OSN wants to publish and hand over this data to any third party for research or commercial purposes. However, at the same, the OSN wishes to maintain the privacy of its users. In this case, the OSN applies anonymization techniques to preserve user privacy. The second term is the 'privacy protection' and it is used in situations when the end user even does not want to share their data with the OSN server. In this case, security techniques are used to protect the privacy of users. Our focus is on privacy but at the same time the security techniques that are used to protect user privacy, so security and privacy terms are used throughout the article.

2. Motivation

The motivational factor behind this work is to give a brief overview of raised privacy and security issues due to the use of OSNs. This is a fact that is necessary for everyone to use one a technological

facility for smooth and fast communication. Social media are one type of these communications that have both negative and positive effects to their users. OSNs make information sharing more convenient and rapid than real-life communications. They make globalization a reality and provide a chance to their users to express themselves. OSNs are also a new way for international relationships, whether the relationship is related to business or social interactions. It is easy for people to interact with each other using OSNs anytime and anywhere in the world. Along with these advantages, social media have disadvantages, one of which being the issue of privacy and security. In this paper, the issues that can harm OSN users are discussed, in addition to giving them recommendations on how to protect their privacy while using OSNs.

The rest of the paper is organized as follows. Section 3 gives an overview of the privacy and security threats in OSNs. Section 4 provides the results and discussions of the questionnaire. Section 5 provides recommendations for the protection of user contents and privacy from unauthorized access, and Section 6 concludes the paper.

3. Privacy and Security Threats in OSNs

User-generated content on social media may include users' experiences, opinions, and knowledge. In addition, it may also include private data, for example, name, gender, location, and private photos [7]. Online-shared information is electronically stored and is therefore permanent, replicable, and reshareable [8]. OSN users generally face the challenges of managing their social identity while compromising their social privacy. The popularity of social media is such that worldwide active users of social media are expected to reach around 2.95 billion by 2020, which is about one third of the world's entire population (https://www.statista.com/topics/1164/social-networks/). The total active users on different popular social media networks are presented in Table 1 (https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/).

Table 1. Popular Online Social Networks (OSNs) and their total active users in millions.

OSN	Total Active Users in Millions
Facebook	2047
YouTube	1500
WhatsApp	1200
WeChat	938
Instagram	700
Twitter	328
Skype	300
Viber	260

Taking into account this global number of users, privacy is one of the obvious and critical issues regarding OSNs. Various privacy issues are fostered because of OSNs, such as surveillance, in which the social sphere of OSNs changes to a commercial sphere and OSN service providers supervise user actions for market force access control. Standard OSNs share users' personal data with third parties for advertisement purposes that may be exploited [9]. Likewise, OSN users leave digital imprints when they browse OSN sites, and therefore are targeted as data sources for commercial uses and user profiling.

Social-networking tools have changed the way we interact in our personal and professional lives. Although they play a significant role in our social and business lives, at the same time they bring about high risks concerning privacy and security. As hundreds of thousands of users use OSNs on a regular basis, they have attracted the attention of attackers more than any other target in recent years. Because of the high usage of social media, online users have been exposed to privacy and security threats. These threats can be categorized into classic and modern threats. Classic threats are online threats that not only make OSN users vulnerable, but also other online users who do not use any OSN. The second type of threats is modern threats, which are related to OSN users only

because of the OSN infrastructure that can compromise user privacy and security [10]. A 2016-based finding, NopSec, the State Vulnerability Risk Management Report (http://info.nopsec.com), claims that organizations are using inadequate risk-evaluation scoring systems. The report states that social media are not included in the risk-evaluation scoring system but they are one of the top types of platform for cybersecurity.

3.1. Classic Threats

Classic threats have been an issue ever since the development of the Internet. These threats are spam [11], malware [12], phishing [13], or cross-site scripting (XSS) attacks [14]. Although researchers and industries have addressed these threats in the past with the invention of OSNs, they can spread in a new way and more quickly than ever before. Classic threats are used to extract the personal information of users, which are shared through an OSN, not only to attack the target users but also their peers by adjusting the threat to correlate to users' private attributes.

3.1.1. Malware

Malware stands for malicious software. It is a generic term that refers to intrusive software. It is developed with the intention to log into someone's computer and access their private contents. A malware attack on social networks is easier as compared to other online services because of the structure of an OSN and the interactions among users. The worst malware case is to access users' credentials and impersonate them to send messages to their peers. For example, the Koobface malware was spread through OSNs such as MySpace, Facebook, and Twitter. It was used to collect login credentials and make the target-infected computer a part of a botnet [15]. An OSN has a vital role for various purposes, for example, marketing and entertainment. However, it has opened up its users to harmful activities. Committing fraud and propagating malware are criminal actions wherein users are engaged to access a URL and run a malicious code on the computer of an OSN user [16].

3.1.2. Phishing Attacks

Phishing is another type of fraudulent attack in which the intruder acquires the user's personal information by masquerading as a trustworthy third party through either a fake or stolen identity. For example, during an attack that was attributed to intelligence by the Chinese government, senior U.K. and U.S. military officials were tricked into becoming Facebook 'friends' with someone impersonating the U.S. Navy Admiral James Stavridis [17]. Similarly, social media were used in many places by phishers posing as other persons [18–20].

3.1.3. Spam Attacks

Spam messages are unwanted messages. In OSNs, spam comes as a wall post or a spam instant message. Spam in OSNs is more dangerous as compared to traditional email spam because users spend more time on OSNs. Spam messages normally contain advertisements or malicious links that can lead to phishing or malware sites. Generally, spam comes from fake profiles or spam applications. In case of a fake profile, it is normally spread from a profile created in the name of a popular person [21]. Spam messages normally come from compromised accounts and spamming bots [22]. However, the majority of spam spreads from compromised accounts [23,24]. Spam-filtering approaches are used to detect a malicious message or URL in a message and filter it before delivering it to the target system [25,26].

3.1.4. Cross-Site Scripting

XSS is a vulnerable attack on web-based applications. It is one of the most common and serious security problems that drastically affect web applications [27]. An XSS attack allows an intruder to run malicious code on the targeted user's web browser that results in compromised data, theft of

data stored in the form of cookies, and saving passwords and credit-card numbers. Furthermore, an attacker can use XSS with a social-network infrastructure and develop an XSS worm that can be virally spread on OSNs [28].

3.2. Modern Threats

These threats are typically related to OSNs. Normally, the focus of modern threats is to obtain the private information of users and their friends, for example, an attacker wishes to know about a user's current employer information. If users have their privacy setting on their Facebook account as public, they can be easily viewed. However, if they have the customized privacy setting, then it is viewable to their friends only. In this situation, the attacker can create a Facebook profile and send a friend request to targeted users. Upon acceptance of the friendship request, details are disclosed to the attacker. Similarly, the intruder can employ an inference attack to collect users' personal information from their peers' publicly available contents.

3.2.1. Clickjacking

Clickjacking is also known as a user-interface redress attack, wherein a malicious technique is used to make online users click on something that is not the same for which they intend to click. In clickjacking attacks, an attacker can manipulate OSN users into posting spam posts on their timeline and asks for 'likes' to links unknowingly. With a clickjacking attack, attackers can even use the hardware of user computers, for example, a microphone and camera, to record their activities [29].

3.2.2. De-anonymization Attacks

De-anonymization is a strategy based on data-mining techniques, wherein unidentified information is cross-referenced with public and known data sources to reidentify an individual in the anonymous dataset. OSNs provide strong means of data sharing, content searching, and contacts. Since the data shared through OSNs are public by default, they are an easy target for deanonymization attacks [30]. In existing online services, pseudonyms are used for data anonymity to make the data publicly available. However, there are several deanonymization techniques to reidentify an individual from such data. For example, a recent work [31] claims a precise and robust deanonymization attack on social-network data.

3.2.3. Fake Profiles

A typical attack in most of the social networks is a fake-profile attack. In this kind of attack, an attacker creates an account with fake credentials on a social network and sends messages to legitimate users. After receiving friendship responses from users, it sends spam to them. Usually, fake profiles are automated or semiautomated and mimic a human. The goal of the fake profile is to collect the private information of users from the OSN, which is accessible only to friends, and spread it as a spam. The fake-profile attack is also a problem for the OSN service providers because it misuses their bandwidth [32]. Moreover, it can be used for various purposes, for example, advertisements. Making fake followers and retweets is a large IT business, and it is possible because of fake profiles [33], but it gives misleading information to viewers.

3.2.4. Identity Clone Attacks

Profile cloning can be performed by an attacker using theft credentials from an already existing profile, creating a new fake profile while using stolen private information. These attacks are known as identity clone attacks (ICAs) [34]. The stolen credentials can be used within the same network or across different networks. The attacker can use the trust of the cloned user to collect contents from their peers or perform different types of online fraud [35].

3.2.5. Inference Attacks

Inference attacks on social networks are applied to predict the sensitive and personal information of a user that they may not want to disclose, for example, age, gender, religious, and political affiliations. The attributes or information that are revealed inside the network are supposed to be private, but it is possible to use data-mining techniques on the released OSN data to predict a user's private information. Machine-learning algorithms can be applied for inference attacks by combining publicly available social-network data, for example, network topology and contents from users' peers. A mutual-friend-based attack can be used to find the common neighbor of any two users [36]. An inference attack was presented in Reference [37] to predict the attributes of a user based on their other public attributes that were available online. The technique was tested on Facebook to infer different users' attributes, such as educational background, preferences, and location information.

3.2.6. Information Leakage

Social media are all about openly sharing and exchanging information with friends. Some users willingly share their personal informationm such as health-related data [38]. Unfortunately, a few of them share a bit too much personal information about products, projects, organization, or any other kind of private data. The sharing of such sensitive and private content may have negative implications for OSN users. For instance, an insurance company may dig in OSN data to classify users as risky clients [39].

3.2.7. Location Leakage

The location-leakage threat is a type of data leakage. There is a trend for various users to access a social network through mobile devices. Usually, apps are used to access an online source through a mobile device. The use of mobile devices for online access introduces the new privacy threat of location leakage. The use of mobile devices for online access encourages users to share their location information [40]. Thus, the revealing of geographic data on social-networking sites may be used by attackers to harm users.

3.2.8. Cyberstalking

Cyberstalking is to harass an individual or group through the Internet or social networking. It could be used for monitoring, identity theft, threats, solicitation for sex, or harassment [41]. Winkelman et al. [42] worked on the study to examine women's experiences with cyberharassment and their attitudes toward it using an anonymous online survey. A total of 293 women were asked, where the participants of the survey were selected from different OSN sites in their research. A good percentage of participants, i.e., 58.5%, were students at a college or university. Almost 20% of women repeatedly received sexual messages or sexual solicitations on the Internet. Approximately 10% received pornographic messages from some unknown users, whereas more than 33% of them experienced cyberharassment.

3.2.9. User Profiling

User profiling is one of the common activities in almost all online services, where OSN servers analyze routine user activities in their space through various machine-learning techniques. User profiling has some advantages for recommending required objects to users. However, it may lead to privacy leakage because user profiles contain personal information. Therefore, user profiling is a privacy issue and its protection is needed in an OSN environment. Online service providers perform user profiling for commercial purposes; however, it can open up the way for privacy leakage [43].

3.2.10. Surveillance

Social-media surveillance is a new type of monitoring that is different from the sociability and social roles of a person in politics, the economy, and civil society. It becomes a process for monitoring the various activities of their users in different social roles by using their profiles and relationships with others. Social-media surveillance is a technology-based surveillance in which human activities are monitored on social media [44].

4. Results and Discussion

A questionnaire was designed to ask questions from OSN users. Questions were asked from bachelors-level students. The aim of the survey was to know how users treated different types of privacy-related options and whether they knew or cared about these options or not. The participants of the survey were students of bachelor level (sixteen years of education), and they were selected randomly from different classes. The questions that were asked to the various participants of the survey and the responses were disappointing because many of the users even did not use the existing privacy settings offered by service providers. The results of the questionnaire are summarized and shown in Figure 1. The following questions were asked of the participants:

Question: Do you share your personal information on the OSN?

The answers of 23% participants were YES, in that they do share their personal information on OSNs. The participants were further asked whether they restrict their content and only share with friends, Unfortunately, several of them were even not using the limited data-sharing facility offered by the service providers. For example, the OSN provided the facility to only share contents with friends, friends of friends, or custom sharing.

Question: Do you accept more than one friendship request from the same user?

This question was asked to know whether or not users are vulnerable to clone attacks. In a clone attack, the attacker uses theft credentials of an already existing user and creates a new fake profile while using the stolen private information. From participants, 21% responded to this question that YES, they accept the request of users who send a friend request while their friend requests were already been accepted. It does not mean that all these requests are clone attacks, but this shows that these users are vulnerable to clone attacks.

Question: Do you use your real name for your profile?

In this case, 46% of users use their real names as their profile names. It shows their trust in the OSN.

Question: Do you use your real picture as a profile photo?

Here, 45% of the survey participants responded that they use their real pictures as their profile photos. The photos are somewhat personal data, and if a user keeps the profile picture as a real one, they may share more personal photos on the OSN.

Question: Do you read the terms of use or privacy statement of your OSN?

The users were asked about the privacy statement of their OSN, where 54% of them even did not try to read the terms of use of their OSNs. The rest of the participants read some portion of the privacy statement. The privacy statement is too much long, which is almost difficult for a user to read it in a short time. However, most of the users directly accept that without even reading it. Even if users read it and they may not like some sentences, they cannot change it. Thus, they may either accept it or cannot use the services without accepting the terms of use statement.

Question: Do you regularly change your password ?

Login ID and password are used to log into an OSN. Sometimes, a password may be compromised due to any reason. In such a case, the password needs to be changed in order to protect the user

account from unauthorized access. Therefore, every user needs to regularly change the password. In our survey, 42% of the participants did not change their passwords regularly.

Question: Do you customize your privacy settings?

Almost every OSN provides some level of access control to their users. Users can restrict the access to their contents by using the customized access control mechanism provided by OSNs. However, 43% of users did not even use the existing privacy settings provided by the OSNs.

Question: Do you have any password on your mobile device that you use for social networking?

Currently, many of the users use their mobile devices for social networking. Normally, apps are used for this purpose. Any person who has access to a mobile device can access all apps installed on it. Therefore, a password is necessary to protect all apps installed on a user mobile. In this survey, 41% of users did not even protect their mobile devices through password protection and keep their mobile devices without password protection.

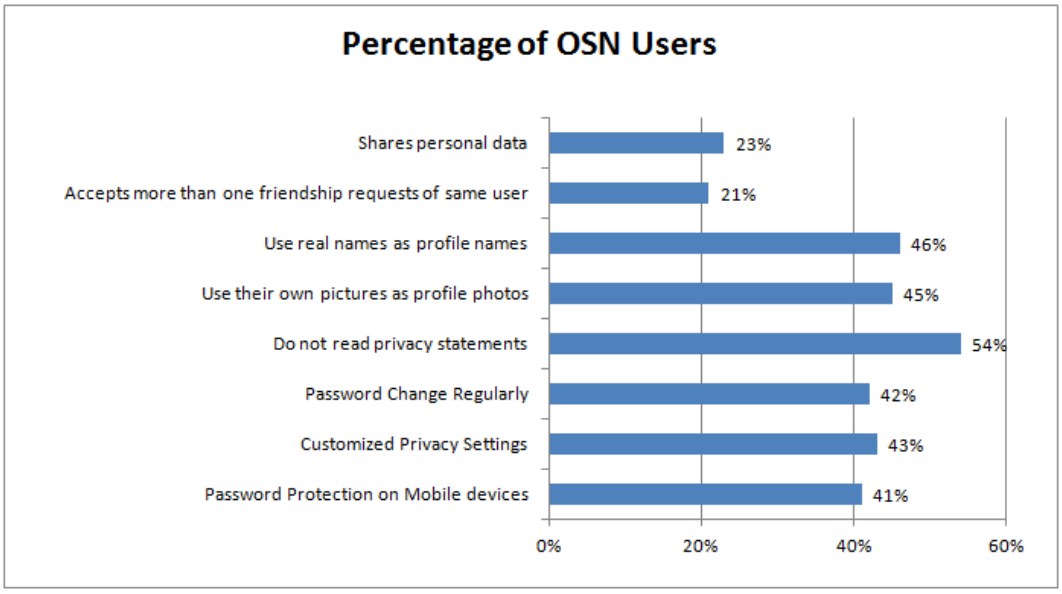

Figure 1. Percentage of users who either do not know or care about their privacy while using OSNs.

5. Recommendations

OSNs have a number of privacy and security issues, but various privacy challenges can be overcome by using precautionary measures. An attacker exploits security and privacy issues in OSNs due to the negligence of users. The contents shared by OSN users with their friends may go to the wrong hands, either in the same format or in a different context. Similarly, contents that are shared can be merged with other public datasets using reidentification techniques where a profile may be reconstructed that can further disclose personal privacy [45]. The frontline defence against such privacy threats is provided through the privacy settings that are controlled by OSNs. However, the effectiveness of these privacy settings is not sufficient because it is designed in the form of an agreement with its users to collect more information from them rather than protecting their privacy. The following are our recommendations for the protection of user contents and the privacy from unauthorized access.

Privacy settings: Regrettably, 80% of users neither check their OSNs nor know about the privacy of their profile whether they have been offered default privacy settings or adequate privacy that meets the expected level [46]. Although OSNs offer a particular level of access control to data owners via customized settings so as to hide contents from unauthorized access, the default

privacy settings of almost all OSNs have restrained privacy [47]. Different social-network users keep the default security and privacy settings [48,49]. OSN users are recommended to keep customized privacy settings and take maximum advantage of the privacy-protection techniques provided by their OSNs. Similarly, users are advised to frequently revise their privacy settings because various OSNs change their privacy settings after every update.

Personal Information: Once contents are shared through any third party, there is no guarantee that these contents would be private anymore. Therefore, users are required to avoid sharing unnecessary private data on OSNs. Even though a user might understand the importance of privacy, the privacy policies provided by the OSNs often create confusion about the privacy of contents that a user shares on them [50]. For example, research found that 94% of users were sharing contents on OSNs that were intended to be private [51].

Location Information: A number of mobile apps collect user-location information. This location information can be used by OSNs and may be provided to third parties, primarily for commercial purposes, which leads to privacy leakage. Individuals cannot use such type of location information collected by OSNs, but they often share their locations with their posts. Attackers can misuse this location information by knowing your current place. Therefore, users are recommended to not disclose their location information through OSNs in order to be safe from these potential attackers.

Antivirus and Antispyware: An OSN is one of the leading means of communication between individuals where content distribution can be easily done [52]. Using the nature of content dissemination through OSNs, malware distribution has grown exponentially [53,54]. Malware is any type of malicious software used to disrupt user operations, illegally gather sensitive information, gain unauthorized access to private data, or inconvenience users through unwanted advertising pop-ups [55,56]. OSN users are recommended to install antivirus and antispyware software on their computers/mobile phones to counter these types of malware and spyware.

Third-Party Applications: Third-party apps give rise to a number of privacy and security issues because their code is hosted outside the OSN and user controls. This inherently prevents the OSN and users from controlling and monitoring the app's activities, and to take proactive measures to stop malicious penetration. Since the data are transferred out of the OSN, the utilization of user contents and their distribution is not in the control of the users [57]. Thus, they are required to uninstall third-party applications to protect their information that can go into the wrong hands.

6. Conclusions

Social media have a number of advantages, but along with these benefits, OSNs have raised some issues related to them. The security and privacy of users and their data are the core issues related to social media. These issues could occur from OSN service providers, unauthorized users, or third parties that use OSN data for their businesses. In this paper, different privacy and security issues associated with OSN users and data from OSN service providers, as well as third-party data collectors, are explained. The main purpose of the study was to educate OSN users on how to protect themselves from these issues whenever they use social media.

Author Contributions: S.A. and N.I. conceived and designed the experiments; A.R. performed the experiments; I.U.D. and M.G. analyzed the data; J.J.P.C.R. contributed the reagents, materials, and analysis tools; and S.A. and I.U.D. wrote the paper.

Acknowledgments: This work is supported by the National Funding from the FCT-Fundação para a Ciência e a Tecnologia through the UID/EEA/500008/2013 Project; by Finatel through the Inatel Smart Campus project; by Finep, with resources from Funttel, grant no. 01.14.0231.00, under the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações—CRR) project of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações—Inatel), Brazil; by Brazilian National Council for Research and Development (CNPq) via Grant No. 309335/2017-5.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Boyd, D.M.; Ellison, N.B. Social network sites: Definition, history, and scholarship. *J. Comput.-Mediat. Commun.* **2007**, *13*, 210–230. [CrossRef]
2. Obar, J.A.; Wildman, S. Social media definition and the governance challenge: An introduction to the special issue. *Telecommun. Policy* **2015**, *39*, 745–750. [CrossRef]
3. Kaplan, A.M.; Haenlein, M. Users of the world, unite! The challenges and opportunities of Social Media. *Bus. Horiz.* **2010**, *53*, 59–68. [CrossRef]
4. Shozi, N.A.; Mtsweni, J. Big data privacy in social media sites. In Proceedings of the 2017 IST-Africa Week Conference (IST-Africa), Windhoek, Namibia, Southern Africa, 30 May–2 June 2017; pp. 1–6.
5. Nissenbaum, H. Privacy as Contextual Integrity. *Wash. L. Rev.* **2004**, *79*, 101–139.
6. Davison, H.K.; Maraist, C.C.; Hamilton, R.; Bing, M.N. To Screen or Not to Screen? Using the Internet for Selection Decisions. *Empl. Responsib. Rights J.* **2012**, *24*, 1–21. [CrossRef]
7. Taddicken, M. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *J. Comput.-Mediat. Commun.* **2014**, *19*, 248–273. [CrossRef]
8. Marwick, A.E.; Boyd, D. Networked privacy: How teenagers negotiate context in social media. *New Media Soci.* **2014**, *16*, 1051–1067. [CrossRef]
9. Ashtari, S. I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy. *J. Inf. Priv. Secur.* **2013**, *9*, 80–82. [CrossRef]
10. Fire, M.; Goldschmidt, R.; Elovici, Y. Online social networks: Threats and solutions. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 2019–2036. [CrossRef]
11. Heymann, P.; Koutrika, G.; Garcia-Molina, H. Fighting spam on social web sites: A survey of approaches and future challenges. *IEEE Internet Comput.* **2007**, *11*, 36–45. [CrossRef]
12. Everett, C. Social media: Opportunity or risk? *Comput. Fraud Secur.* **2010**, *2010*, 8–10. [CrossRef]
13. Alarm, S.; El-Khatib, K. Phishing Susceptibility Detection through Social Media Analytics. In Proceedings of the 9th International Conference on Security of Information and Networks, Newark, NJ, USA, 20–22 July 2016; pp. 61–64.
14. Nithya, V.; Pandian, S.L.; Malarvizhi, C. A survey on detection and prevention of cross-site scripting attack. *Int. J. Secur. Appl.* **2015**, *9*, 139–152. [CrossRef]
15. Baltazar, J.; Costoya, J.; Flores, R. The Real Face of Koobface: The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research. 2009. Available online: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_the-real-face-of-koobface.pdf (accessed on 21 October 2018).
16. Alghamdi, B.; Watson, J.; Xu, Y. Toward detecting malicious links in online social networks through user behavior. In Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence Workshops, Omaha, NE, USA, 13–16 October 2016; pp. 5–8.
17. Protalinski, E. Chinese Spies Used Fake Facebook Profile to Friend Nato Officials. Available online: https://www.zdnet.com/article/chinese-spies-used-fake-facebook-profile-to-friend-nato-officials/ (accessed on 21 October 2018).
18. Dvorak, J.C. LinkedIn Account Hacked. Available online: https://www.pcmag.com/article2/0,2817,2375983,00.asp (accessed on 1 November 2018).
19. Miller, S. Sen. Grassley's Twitter Account Hacked by SOPA Protesters. Available online: https://abcnews.go.com/blogs/politics/2012/01/sen-grassleys-twitter-account-hacked-by-sopa-protesters/ (accessed on 1 November 2018).
20. Vishwanath, A. Getting phished on social media. *Decis. Support Syst.* **2017**, *103*, 70–81. [CrossRef]
21. Fire, M.; Katz, G.; Elovici, Y. Strangers intrusion detection-detecting spammers and fake profiles in social networks based on topology anomalies. *Human J.* **2012**, *1*, 26–39
22. Egele, M.; Stringhini, G.; Kruegel, C.; Vigna, G. Towards detecting compromised accounts on social networks. *IEEE Trans. Dependable Secure Comput.* **2017**, *14*, 447–460. [CrossRef]
23. Grier, C.; Thomas, K.; Paxson, V.; Zhang, M. @spam: The underground on 140 characters or less. In Proceedings of the 17th ACM conference on Computer and Communications Security, Chicago, IL, USA, 4–8 October 2010; pp. 27–37.

24. Gao, H.; Hu, J.; Wilson, C.; Li, Z.; Chen, Y.; Zhao, B.Y. Detecting and characterizing social spam campaigns. In Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement, Melbourne, Australia, 1–3 November 2010; pp. 35–47.
25. Thomas, K.; Grier, C.; Ma, J.; Paxson, V.; Song, D. Design and evaluation of a real-time URL spam filtering service. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 22–25 May 2011; pp. 447–462.
26. Gao, H.; Chen, Y.; Lee, K.; Palsetia, D.; Choudhary, A.N. Towards Online Spam Filtering in Social Networks. In Proceedings of the 19th Annual Network & Distributed System Security Symposium, San Diego, CA, USA, 5–8 February 2012; pp. 1–16.
27. Gupta, S.; Gupta, B.B. Cross-Site Scripting (XSS) attacks and defense mechanisms: Classification and state-of-the-art. *Int. J. Syst. Assur. Eng. Manag.* **2017**, *8*, 512–530. [CrossRef]
28. Faghani, M.R.; Nguyen, U.T. A study of XSS worm propagation and detection mechanisms in online social networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 1815–1826. [CrossRef]
29. Lundeen, R.; Ou, J.; Rhodes, T. New Ways Im Going to Hack Your Web APP. Black Hat Abu Dhabi. Available online: https://www.blackhat.com/html/bh-ad-11/bh-ad-11-archives.html#Lundeen (accessed on 1 November 2018).
30. Ding, X.; Zhang, L.; Wan, Z.; Gu, M. A brief survey on de-anonymization attacks in online social networks. In Proceedings of the IEEE International Conference on Computational Aspects of Social Networks (CASoN 2010), Taiyuan, China, 26–28 September 2010; pp. 611–615.
31. Gulyás, G.G.; Simon, B.; Imre, S. An Efficient and Robust Social Network De-anonymization Attack. In Proceedings of the Workshop on Privacy in the Electronic Society, Vienna, Austria, 24 October 2016; pp. 1–11.
32. Wani, M.A.; Jabin, S.; Ahmad, N. A sneak into the Devil's Colony-Fake Profiles in Online Social Networks. Available online: https://arxiv.org/ftp/arxiv/papers/1705/1705.09929.pdf (accessed on 29 October 2018).
33. Perlroth, N. Fake Twitter Followers Become Multimillion-Dollar Business. *The New York Times*, 9 April 2013. Available online: https://bits.blogs.nytimes.com/2013/04/05/fake-twitter-followers-becomes-multimillion-dollar-business/?_php=true&_type=blogs&ref=technology&_r=0 (accessed on 1 November 2018).
34. Kharaji, M.Y.; Rizi, F.S.; Khayyambashi, M.R. A New Approach for Finding Cloned Profiles in Online Social Networks. *arXiv*, **2014**, arXiv:1406.7377.
35. Lewis, J. How spies used Facebook to Steal NATO Chief's Details. *The Telegraph*, 10 March 2012.
36. Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. Preventing private information inference attacks on social networks. *IEEE Trans. Knowl. Data Eng.* **2013**, *25*, 1849–1862. [CrossRef]
37. Viswanath, B.; Bashir, M.A.; Crovella, M.; Guha, S.; Gummadi, K.P.; Krishnamurthy, B.; Mislove, A. Towards Detecting Anomalous User Behavior in Online Social Networks. In Proceedings of the USENIX Security Symposium, San Diego, CA, USA, 20–22 August 2014; pp. 223–238.
38. Torabi, S.; Beznosov, K. Privacy Aspects of Health Related Information Sharing in Online Social Networks. In Proceedings of the 2013 USENIX Conference on Safety, Security, Privacy and Interoperability of Health Information Technologies, Washington, DC, USA, 12 August 2013; p. 3.
39. Scism, L.; Maremont, M. Insurers Test Data Profiles to Identify Risky Clients. *The Wall Street Journal*, 19 November 2010.
40. Humphreys, L. Mobile social networks and social practice: A case study of Dodgeball. *J. Comput.-Mediat. Commun.* **2007**, *13*, 341–360. [CrossRef]
41. D'Ovidio, R.; Doyle, J. A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforc. Bull.* **2003**, *72*, 10–17.
42. Burke Winkelman, S.; Oomen-Early, J.; Walker, A.D.; Chu, L.; Yick-Flanagan, A. Exploring Cyber Harassment among Women Who Use Social Media. *Univers. J. Public Health* **2015**, *3*, 194–201. [CrossRef]
43. Ali, S.; Rauf, A.; Islam, N.; Farman, H.; Khan, S. User Profiling: A Privacy Issue in Online Public Network. *Sindh Univ. Res. J. (Sci. Seri.)* **2017**, *49*, 125–128.
44. Fuchs, C.; Trottier, D. Towards a theoretical model of social media surveillance in contemporary society. *Commun. Eur. J. Commun. Res.* **2015**, *40*, 113–135. [CrossRef]
45. Gross, R.; Acquisti, A. Information revelation and privacy in online social networks. In Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society, Alexandria, VA, USA, 7–10 November 2005; pp. 71–80.

46. Zhang, W.; Al Amin, H. Privacy and security concern of online social networks from user perspective. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP2015), ESEO, Angers, Loire Valley, France, 9–11 February 2015; pp. 246–253.
47. Carminati, B.; Ferrari, E.; Heatherly, R.; Kantarcioglu, M.; Thuraisingham, B. Semantic web-based social network access control. *Comput. Secur.* **2011**, *30*, 108–115. [CrossRef]
48. Strater, K.; Richter, H. Examining privacy and disclosure in a social networking community. In Proceedings of the 3rd Symposium on Usable Privacy and Security, Pittsburgh, PA, USA, 18–20 July 2007; pp. 157–158.
49. Miltgen, C.L.; Peyrat-Guillard, D. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *Eur. J. Inf. Syst.* **2014**, *23*, 103–125. [CrossRef]
50. Fletcher, D. How Facebook Is Redefining Privacy. Available online: http://content.time.com/time/magazine/article/0,9171,1990798,00.html (accessed on 10 November 2018).
51. Madejski, M.; Johnson, M.; Bellovin, S.M. A study of privacy settings errors in an online social network. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, Switzerland, 19–23 March 2012; pp. 340–345.
52. Penni, J. The future of online social networks (OSN): A measurement analysis using social media tools and application. *Telemat. Inform.* **2017**, *34*, 498–517. [CrossRef]
53. Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. Design and analysis of a social botnet. *Comput. Netw.* **2013**, *57*, 556–578. [CrossRef]
54. Makridakis, A.; Athanasopoulos, E.; Antonatos, S.; Antoniades, D.; Ioannidis, S.; Markatos, E.P. Understanding the behavior of malicious applications in social networks. *IEEE Netw.* **2010**, *24*, 14–19. [CrossRef]
55. Tam, K.; Feizollah, A.; Anuar, N.B.; Salleh, R.; Cavallaro, L. The evolution of android malware and android analysis techniques. *ACM Comput. Surv.* **2017**, *49*, 76. [CrossRef]
56. Provos, N.; McNamee, D.; Mavrommatis, P.; Wang, K.; Modadugu, N. The Ghost in the Browser: Analysis of Web-based Malware. In Proceedings of the First Workshop on Hot Topics in Understanding Botnets (HotBots'07), Cambridge, MA, USA, 10 April 2007; p. 4.
57. Chaabane, A.; Ding, Y.; Dey, R.; Kaafar, M.A.; Ross, K.W. A Closer Look at Third-Party OSN Applications: Are They Leaking Your Personal Information? In Proceedings of the 15th International Conference on Passive and Active Network Measurement, Los Angeles, CA, USA, 10–11 March 2014; pp. 235–246.