Social Networks' Benefits, Privacy, and Identity Theft: KSA Case Study

Ahmad A. Al-Daraiseh
dep. Information System
King Saud University, KSA
Riyadh, Saudi Arabia

Afnan S. Al-Joudi
dep. Information System
King Saud University, KSA
Riyadh, Saudi Arabia

Hanan B. Al-Gahtani
dep. Information System
King Saud University, KSA
Riyadh, Saudi Arabia

Maha S. Al-Qahtani
dep. Information System
King Saud University, KSA
Riyadh, Saudi Arabia

***Abstract*—Privacy breaches and Identity Theft cases are increasing at an alarming rate. Social Networking Sites (SN's) are making it worse. Facebook (FB), Twitter and other SN's offer attackers a wide and easily accessible platform. Privacy in the Kingdom of Saudi Arabia (KSA) is extremely important due to cultural beliefs besides the other typical reasons. In this research we comprehensively cover Privacy and Identity Theft in SNs from many aspects; such as, methods of stealing, contributing factors, ways to use stolen information, examples and other aspects. A study on the local community was also conducted. In the survey, the participants were asked about privacy on SN's, SN's privacy policies, and whether they think that SN's benefits outweigh their risks. A social experiment was also conducted on FB and Twitter to show how fragile the systems are and how easy it is to gain access to private profiles. Results from the survey are scary: 43% of all the accounts are public, 76% of participants do not read the policies, and almost 60% believe that the benefits of SN's outweigh their risks. Not too far from this, the results of the experiment show that it is extremely easy to obtain information from private accounts on FB and Twitter.**

Keywords—social network; identity theft; fraud; privacy; fake identities

I. Introduction

Computer technology and the Internet have become essential necessities of modern life; they provide knowledge, communications, entertainment, and a means for sharing. Nowadays, almost everyone is connected. People became so addicted to this technology to the limit that it is a challenge now to stay away for a while. Perhaps the most attractive services for many are those provided by social networks.

Social Networks (SN) are Internet based services that allow people to interact, express and share their ideas and thoughts in multiple formats; such as, text, images, audio, and video. Although still young, SN's gained large popularity. As of Sep 2014, Facebook (FB) prides itself for having more than 860 million active users daily [1]. When using SN's, different people share different amounts of their personal information. Having our personal information fully or partially exposed to the public, makes us ideal targets for different types of attacks, the worst of which could be identity theft.

Identity theft occurs when someone uses another person's information for a personal gain or goal. During the past years, online identity theft has been a major problem since it affected millions of peoples around the world [2]. Victims of identity theft may suffer different types of consequences; for example, they might lose time/money, get sent to jail, get their public image ruined, or have their relationships with friends and family broken.

Today, the majority of SN's do not verify normal users' accounts and have very weak privacy and security policies. In fact, most SN's applications default their settings to minimal privacy; and hence, SN's became an ideal platform for fraud and abuse. Social Networking services have facilitated identity theft and Impersonation attacks for serious as well as naive attackers. To make things worse, users are required to provide accurate information to establish an account in Social Networking sites. Simple monitoring of what users share online could lead to catastrophic losses, let alone, if such accounts were hacked.

In this article, we shed a light on the benefits and risks associated with SN's. We study the local community in the Kingdom of Saudi Arabia (KSA) to see if the benefits of SN's outweigh their risks and dangers. Knowing that, Saudi communities are amongst the most protective in the whole world, yet have indulged deeply into the usage of SN's.

A. KSA at a Glance

The Internet first emerged in KSA in 1990. According to the latest statistics and global studies presented by many competent authorities, KSA currently is in the forefront of international rankings in terms of the use of FB and Twitter. There are 100 thousand Tweets per minute and up to 20 victims of online identity theft. Another study stated that the number of FB users in KSA was 6 million in 2012, and in 2013, the number reached 7.8 million, with five million of them accessing their accounts from their mobiles [3].

Recently, many people in KSA from different communities became outraged by impersonation and hacking attacks that targeted their SN accounts. Most of the attacks aim to smear a person or ruin his/her image, others tried to disseminate lies and/or mislead the facts to acquire a large number of followers. In 2013, "AlSharq Newspaper" published an article stating that 35 persons stole a famous Saudi actor's identity in Twitter. Most of them had more than 30 thousand followers, some of them reached 50 thousand, and few reached 80 thousand followers. The fake accounts were used to disseminate lies and to publish undesirable images [4].

The laws in KSA set penalties for anyone who commits any cybercrimes; such as, breaking into websites, or accessing the material sent over the Internet. In Saudi laws, a penalty of up to three million Saudi Riyal, and imprisonment of up to four years for any person who uses unauthorized access to private information [5].

The rest of the paper is organized as follows: In section 2, related work is discussed. In section 3, the methodology is presented. In section 4, a comprehensive study of SN's and Identity Theft is provided. In section 5, Results are analyzed. In sections 6 and 7 Recommendations and conclusions are listed respectively.

II. Related Work

Previously, several researchers published and highlighted the SN's benefits and issues. In the following, few paragraphs we provide a summary of the most recent related work.

M. Reznik [6] published a paper about the identity theft in SN's and methods of Internet impersonation. Maksim discussed two methods that an offender may use to steal the identity of victims on the internet: Firstly, when the offender creates a fictitious profile of the victim and uses it without the victim's permission, secondly, when the offender gains unauthorized access to the victim's account by stealing their credentials.

K. Krombholz et al. [7] reported that one of the main issues in social media is information accuracy. Many FB profiles are fake because many users use false information when they create their profiles. FB rules stated that the user should provide real information to prevent fake identities. The author also said that, to prevent users diverting; FB priority should be safety of their users.

F. Stutzman and J. Kramer-Duffield [8] provide advice on how to enhance the privacy of users in SN's. In order to avoid identity theft, they suggest making users profiles private for friends only, which will reduce the information theft risks on SN's.

A. Verma et al. [9] found that the architecture of centralized SN's such as the current ones don't ensure the privacy and security of the users. Therefore, they proposed a decentralized and distributed architecture that preserves privacy and security of the users in online SN's. This architecture is based on the decentralized SN's using "Freedom box" as a personal server. It uses Diaspora as a social platform. Therefore, each user has a Freedom box to store his/her personal information. They enhanced the privacy and security by the use of a cryptographic technique like (Random Sequence Algorithm) RSA and digital signatures.

L. Bilge et al. [10] examined how easy for an attacker to start automated crawling and identity theft attacks in popular SN's sites to access user personal information. They presented two attacks on victims who have public profiles, one for registered users, and the other one for non-registered users. The first attack is called automated identity theft. In this attack, the authors created cloned victims' profiles then sent friend requests to the contacts of those victims. The second attack is launched an automated cross-site profile cloning attack. In this attack, the attacker can automatically create a forged profile in SN's where the victim is not registered yet, and reach the victim's friends who registered on both networks. The experimental results show that the automated attacks are effective and feasible in practice.

M. Al-Mujeb [11] reviews the relationship between KSA culture and privacy and FB privacy risks. The aim was to know how the KSA's cultural privacy norms affect the user's behavior in FB. She concluded that ''the most participants who are active users of FB are not aware of many of the privacy risks that can arise from sharing personal information and the potential consequences of this, such as stalking, theft and credit card fraud''. The results confirmed, "The users were unaware of the privacy setting in FB that can help them to protect their privacy". The main recommendation of the thesis was encouraging the user to not accept strangers as friends, never share personal information, limit the information available to "Everyone" and read the privacy policy with terms of use.

R. Demyati [12] also talked about FB privacy issues. She discussed how FB responded to the privacy concerns and how that response affected its users. The main concerns were whether FB shares users' information with advertisers and who can see users' photos when their friends tag them. As for FB response, they agreed to change some of their privacy policy and refused to change other parts of it. She concluded with some recommendations such as, encouraging the user to read the privacy policy, keep the sensitive information private, do not accept a friend's request from strangers, open a new email account for FB and report any issues to FB team.

C. Marcum et al. [13] defined identity theft as a type of crime; the high growth of technology has provided new methods to steal the personal information of thousands of victims at once. Indeed, the increased number of users on SN's sites, and the relatively weak security and authentication procedures have exacerbated this problem. The research also suggested that users may not understand the risks associated with sharing personal information or the potentiality to use this information to predict highly confidential data like social security numbers.

J. Mali [14] said that in 2012, there were more than 12 million victims of identity theft in the US. Many financial institutions and companies are enforcing measures to protect their customers, but criminals explore new ways to collect sensitive data through SN. FB claimed that users data was safe, while Twitter suffered an attack were more than 250,000 accounts were affected.

B. Pragides [15] found that most of identity theft cases occur to the younger generation because they use SN's as a way to communicate with friends and to make new relationships with new people.

Up to our knowledge, no one comprehensively studied SN's and identity theft, or provided a field study to measure the impact of risks on users' usage of such services; and hence, this paper is unique as it fully and exclusively covers SN's issues in KSA.

III. Methodology

In this research, we focus on finding and analyzing the reasons of identity theft in SN's and the prevalent plans for handling identity theft related to it. We discuss the answers of the following questions: To what extent do users trust SN's sites? Are the SN's sites a safe place to share personal information? Do the advantages of SN's outweigh the risk of identity theft in KSA?. To find and understand the answers, we did a field study to examine the qualitative outcomes along with the quantitative ones by applying three methods:

- **Data Collection:** We collected the data through an online survey, which was made available to everyone to evaluate their knowledge regarding the privacy and security policies of SN's providers, and to discover their concerns regarding such services.
- **Data Analysis:** After gathering data, we analyzed it to find out what the main reasons for identity theft in SN's are, also, to find out the level of personal information that the user can share on SN's.
- **Social Experiment**: In order to test the confidence and awareness among users of SN's, their knowledge in terms of their security and privacy, and to measure the robustness of FB's and Twitter's privacy measures, we designed a social experiment. In this experiment, we cloned public accounts and sent requests to friends of the original account owner who sat their profiles to private.

IV. Social Networks

Nowadays, SN's gather millions of people who share news, images, and other information. It is clear that SN's have made a significant change in how people communicate and exchange information. A SN is an online service provided by a major company in order to connect users who share the same interests or activity, backgrounds or real-life connections. Most of the SN's are a websites that offer a range of services for their users; such as instant messaging, private messages, blogging, file sharing and other services. The most famous SN's currently are Facebook, Tumblr, Twitter, and Google+.

The social clinic statistics confirms that in 2013, the active users of FB in KSA were 7.8 million users, 26% of whom are females and 74% males [16]. This indicates an increase of 1.8 million users since 2012. Twitter prevalence among Internet users in KSA is the highest worldwide with a total number of 5 million active users and 150 million tweets a day. The number of Twitter users has increased 2 million since 2012 [17].

A. *Social Networks' Benefits*

SN's provide different benefits based on the way they are utilized. The most famous benefits of using social networks in KSA are:

- **Expand the circle of user contacts and acquaintances:** SN's gives users a way to represent themselves. It allows users to form friendships with people from all over the world. Users might find former friends whom they lost connection with.
- **Social networks in education:** SN's can be an excellent tool for education. KSA does not utilize SN's properly for educational purposes yet. Their use in education is limited to individual's efforts and the existence of official profiles representing the Ministry of Education and its leaders.
- **Keep in touch with families and friends:** SN's allow people to share their daily life in a public way. SN's allow families to share events, images, and videos in real time. Family and friends can watch and experience all the things that done individually, and comment on them. They share the experience rather than being informed over a phone call. Pew Research report by Aaron Smith [18] shows that (67%) of social networks users say that the main reason they sing-up in SN's is to keep in touch with their family members and friends. It is a quick way to communicate with relatives and friends who lived in other countries. Some SN's formed a bridge linking the members of the displaced families who were separated by wars and crises of natural disasters.
- **Information gathering and dissemination:** SN's serve as news and media platform, where it can provide news in real time. A user has the agility and mobility at the same time to pass information faster than ordinary news platform. Many Arabs consider SN's a strong competitor to traditional media as SN's stay the main source of news for millions of Arabs. The Arab Social Media Report 2014 [19] shows that nearly 27.59% of the Arab respondents from across the Arab world are getting their news from SN's as the main source. The number of users has increased 21.59% since 2013.
- **Social influence:** SN's are useful in formulating and gathering public opinion, where information can rapidly spread. This impact can vary in its directions. SN's played a big role in the revolutions of the Arab Spring. SN's have all the power to change people opinion, form a protest, or Intercept a public decision. In a report published by foreign policy magazine [20], discusses "The role of new media in moving the masses and more specifically the role of SN's". The writers said, "That SN's are playing a significant and possibly crucial role in empowering rebels and protesters in ways that couldn't have been imagined before". They added, "SN's may be rebels' favorite weapon, but at the same time research on Syria's revolution confirmed that it can do as much harm as good".
- **Finding job opportunities:** The role of SN's is not limited to the social side, but also extends to academic

and professional development. Users can search for job opportunities as the government as well as other companies post job opportunities available in their area. In KSA, users can find specialized profiles that help users find a job that suits their area of interest and specialization.

- **Advertising and generating income:** Companies who have profiles on SN’s can interact with current events that interest the public to use them in their next ads. The release of iPhone 6 is the latest event related to this benefit. In line with what matters to society at the moment, businesses and competing companies took advantage of the bending problem in iPhone 6 in order to promote their products. The influence of SN’s in advertising can be shown more strongly in small business and individuals who work from their home. People, usually, tend to advise their friends to try a successful product they used which helps the individual to build a fan base before expanding their business. As SN’s help in making products attractive, they also can be the cause of the destruction of product reputation for the same reason. There is no room for a compliment because SN’s are the court of the public.

B. *Identity Theft In Social Networks*

Identity theft in SN’s can be done by manipulating people to get sensitive information or by using posts of the victims on SN’s. While SN’s promote sharing amongst users, some people over-share. A large problem with SN’s is that people tend to share a lot of their personal data on their profiles. Such exaggerated sharing makes it easy for identity thieves to do their job. On the other hand, SN’s are facilitating the process for attackers to elicit user personal information and use it in illegal behaviors [7]. Identity thefts in SN’s via social engineering are increasing day after day.

Advertising is one of the main reasons why SN’s require users' personal information. In order to understand why SN’s are free but still encourage users to provide more information, we must first understand how these sites make profits by understanding the advertisements mechanism. Official figures are reporting that 85% of FB profits come from ads [21]. FB profit billions of dollars annually by using the content provided by the users for free. The smart system analyzes all the content shared by the users in order to develop a knowledge base to use it for advertising purposes. Every action taken by the user is used to gather information about him/her; targeted advertisement will then do the job. Information gathered from users via various platforms (i.e. computers, smart phones etc.) is used to form a social graph for each user. Where the user is at the center of the graph and connected to all the entities he is related to by edges. Thus, when a user has 900 million social schemes, the system searches for similarities between them and reclaims general information that benefit in directing advertising campaigns. FB sells this information to third party companies, which often are advertising agencies to use it in campaigns they intend to launch [22]. Given the age of users of SN’s, we can identify another reason for the increase in identity theft in SN’s. Most users are teenagers and young people, who share much of their personal information online with strangers.

1) Methods of stealing information

SN’s provide the biggest platform for the misuse of personal information, and thus, promote frauds and personal data extraction. Therefore, it is not recommended to share the national identity number, driver license number and other important details on such sites; although, some websites require this information from the user [23]. However, sometimes they will not ask directly for this personal data, they will search for related sensitive data then use it in several harmful ways. There are various ways for identity theft to happen [24]:

- **Data Breach:** Organizations and companies store and share all types of sensitive data about their customers. "Data breach" occurs when any of this information is lost by mistake or exposed by the neglected employees.
- **Friendly Fraud:** A high percent of identity theft cases involve friends and family. Most of the victims are young adults and college students because they lack enough knowledge and experience. Hackers can use SN’s, sharing sites, and other shared interests to reach those victim's to steal their personal information. For example, an attacker can know from relative FB page that someone is in a trip to Africa. Depending on this information, he will impersonating his identity and send an email to all the relatives and friends asking them to send money to him due to its exposure to unforeseen circumstances.
- **Computer Hacking:** Cyber criminals are expert at breaking into computers or laptops to steal online banking logins or other financial information.
- **Dumpster Diving:** Dumpster diving is used to retrieve information by searching through the trash for visible treasures in someone else's trash like access passwords or phone list written down on sticky notes.
- **Skimmers:** Devices blend in with ATM machine to collect the credit card information when the card swiped through them. Credit card’s number that was captured by Skimmers’ devices are used to purchase things in the name of the owner of the original card.
- **Stolen Wallet:** Identity theft occurs when the wallet has lost or stolen. Criminals look for everything inside that wallet like driver’s license, bank account numbers, insurance information, and other sensitive information.
- **Mail Theft:** Stealing mail is an easy way for criminals to steal an identity from mailbox or mailbox panels. They know that the mail may contain approved credit offers, loan statements and other information that can use to steal an identity.
- **Shoulder Surfing:** In public places, the best way to see all your confidential and personal information is to look at the screen you are working on behind your back. You never know who is standing behind you or who is

watching you. This method commonly used to obtain user passwords, PINs, and similar information.

- **Account Takeover:** In SN's, when users set their accounts to public it would increase their chances of being victims. Attackers seek to steal personal information of those victims to create fake accounts. An attacker will create a fake account then start to send friend requests to the victim's friends. When a request is accepted, attackers use different techniques to obtain sensitive information from them.

- **Spam Attack:** In SN's, attackers know that users spend more of their time in SN's than on emails. So attackers send spam through SN's by using fake profiles and spam applications that send spam to the friends of the victims [25].

- **Malware:** Malware can spread over SN's by using malicious URL's or by using a fake profile. For example, attackers can create a fake account by using the same name of any famous person and ask victims to contact them, and then attacker can send malware to the victims [25].

- **Spyware:** It is an undesirable program used to collect secretly and record the activities of a person without knowledge of that person. This program loaded through downloading new programs from an unauthorized source.

- **Social Engineering:** The most commonly prevalent identity theft process in KSA. It is a way to gain access to people information without realizing that they are the victim of a security breach using fraud and impersonation. Social engineering is a successful process because the victims tend to be good people, are keen to trust others and tend spontaneously to provide assistance to others. There are many different goals of social engineering hacking, which are fraud, network intrusion, and identity theft disabling systems and networks, and gain unauthorized access to sensitive information. There are several methods of social engineering hacking. For this paper, we will focus on how social engineering is implemented using SN's. Social engineering can be accomplished through the following methods [26]:

- **Online Phishing:** In online phishing, the attackers try to obtain access to the user's sensitive data such as banking information by creating a fake website that looks authentic for a specific bank. Then, attackers send emails and messages to people with a link to a fake website asking them to login for one reason or another.

- **Phone Phishing:** It occurs when the victim receives a call on the phone from people saying they work on trusted bank or company, and they say that that the account need to be updated. In order to update the account, they ask for sensitive information for verification.

- **Romantic Fraud:** This type of fraud frequently occurs through SN's on the Internet. In romantic fraud, attackers rely on stolen images and fake data to the rhythm of their victims from users looking for love and online romance. Continue to deceive victims with stories of love for weeks, and then attackers claim that they need money because of exposure to a tragic accident or injury, and then seek help from the new beloved.

- **Spoofing:** It occurs when an attacker impersonates someone's identity where he can steal credit card information and claiming that the client uses it. Another way of spoofing is when an attacker pretends to be an authorized party or the future party like a bank employee or location to get personal information from the client.

- **Job Posting**: One serious technique used in KSA. The attackers are fake companies or persons who post fake tempting jobs. Desperate unemployed people apply and their data is extracted and used.

2) Factors contributing to identity theft in SN's

The primary profile data that was used by the attacker in order to misuse or steal a user's identity are full name, date of birth, hometown, school info, bank accounts, relationship status and hobbies or interests. Sensitive data can be obtained through GPS enabled devices, like your home address, workplace and places you visit. There are many reasons to keep this information private, because providing this information is potentially dangerous for the user and can put her identity at risk. In KSA, several factors influence and simplify the theft of user's identity on SN's. The main ones are:

- Lack of knowledge on how to protect online identity.

- Lack of knowledge in regulations and cyber laws.

- The overconfidence in the SN provides.

- The enormous expansion in the number of users along with the emerging need of SN's is encouraging the organizations to generate profits using those sites.

- Shortage in knowledge and awareness concerning the privacy policies given by the SN providers.

- Unemployment is a major factor. A large number of unemployed, well-educated youth exist in KSA. Such young people have excellent IT and hacking skills, in addition to all the time they need to perform sophisticated cybercrimes [27].

Currently, these problems are the main focus but policies and laws are being prepared to resolve these concerns. There are different methods and solutions to keep us safe from identity theft. Awareness and knowledge of identity theft and fraud issues are the easiest and cheapest to implement.

3) Fraud and methods of using stolen data

A statistics report published by Trend Micro states that KSA was ranked first as the most vulnerable of the gulf countries to cybercrimes [27]. Identity theft involves stealing and misusing user's identity to gain access to resources or obtaining other profits that are limited to this user. Identity fraud means the usage of a stolen identity to implement criminal behaviors. The problem occurs when a violator has information about someone's identity such as name, current addresses, and date of birth etc., in order to defraud his identity. As it can be done for those who are alive, Identity theft can be performed on the dead. An Identity thief can do many things with the information he has, the most common are:

- **Engage in illegal activities:** If a thief gets caught committing a crime using a stolen identity, the fingerprints and criminal records will put in the victim's name. That will be damaging to the victim’s reputation where the criminal record may cause the victim to fall in the background checks.

- **Obtain a cell phone account**: It happens when identity thieves create a cell phone account using the victim’s stolen information. Then the account charged large bills on the victim’s name.

- **Illegal use of credit card accounts:** The most famous identity theft and the most commonly used process. A burglar gets the victim’s credit card or its information to use it as much as they want on the victim's account. Credit card numbers are usually stolen in bulk from e-commerce businesses; they get sold later on to gangs to be used.

- **Obtaining bank loans:** Frauds can be applied to get loans simply by obtaining a victim’s private data; for e.g. national identity number, address, and work information. Such loans are never paid back, and hence the victim’s credit history will be damaged.

- **Spending victim’s checking and saving accounts:** Thieves can use victim’s personal info to withdraw money from his bank account, transfer savings and take his investments.

- **Get a new ID:** The thieves can use personal information of a live or dead person to create a new ID in their name, but with their images; such as driver’s license.

- **Unauthorized access to utility accounts:** Charging utilities using the victim’s identity; such as Internet, phone, cable, water and electricity utilities. Thieves can open utility accounts using someone's identity simply by extracting little details about the victim.

- **Black market sales:** Hackers use underground online black market for selling the stolen IDs. These black markets are frequently used by hackers around the world to buy the stolen data, or to sell to other hackers locally. Hackers have new ways to make money with SN’s profiles. Researchers at VeriSign’s say that stolen profiles on the FB are now on sale on the black market [28]. Stolen data such as, names, pictures, email addresses, dates of birth are used to create fake profiles. For example, photographs of famous people are used to create false aliases to lure victims [29].

C. Statistics And Examples Of Identity Theft

Statistics show that more than 600,000 FB profiles get compromised each day, were one of six users said that someone hacked their account and stole their identity. Four of ten users have been victims of cybercrime on SN’s, and one of ten users said that they had been a victim to a false link on SN’s. Three of four think that the focusing of cyber criminals is on SN’s platforms. Considering dangerous behavior on SN’s, statistics confirms that one of three users do not log out after sessions. One of five users does not check received links before they share it. One of six users has no clue about their privacy settings if they are public or private. Less than half users use a security tool to defend against SN’s risks and only half of the users use privacy settings to manage the information they share and with whom. Regarding social friends, 36% have accepted friend requests from strangers, and three of ten users received messages from strangers [30].

Communications and Information Technology Commission (CITC) of KSA started a campaign to raise awareness on cybercrimes, but the campaign focused more on the penalties for those crimes [31]. The campaign includes an explanation of the most important types of cybercrimes, and the mechanisms to deal with it. The commission has also established a website called Computer Emergency Response Team [32]. The site goal is to raise the level of awareness, knowledge to detect and response to information security incident at a national level, and to be an official reference for information security in KSA. CITC also established a website called (internet.sa) to be an Internet service gateway in KSA for services, information and statistics references [33]. However, there is no confirmed statistics on the number of identity theft victims on SN’s in KSA; so we decided to go back to the source.

We communicated with a number of experts/hackers and sent them our questions that they answered. In KSA, users can find famous Twitter profiles that can help them at no cost if they lost their account to a hacker. The person behind the profile, usually, had an excellent knowledge in hacking and phishing. They said that the numbers of victims who communicate with them are nearly 150 users a week. From their point of view, their goals in restoring and stealing accounts are noble goals as they consider themselves ethical hackers. Some of them will do it if he sees the accounts interfere with society's values, other do it in order to help the oppressed victim. A lot of Arabs celebrities are seeking their help to restore stolen accounts. Where a many of them did not know that they can contact the technical support team to recover their profiles. On the other side, some hackers do it to sell the accounts, which have large numbers of followers to someone who's interested in making it an advertising account. The fact that SN’s are becoming a potential monetary gain for the hackers is a major threat to users. Particularly for users that do not have a profile on SN’s where some people may use their name in order to make profits by advertising.

Nowadays, almost all companies have official profiles on SN’s. Companies’ representatives manage these profiles. They are constantly conscious about what to post to preserve the company’s public image. Unfortunately, those accounts become targets of unhappy former employees, or angry customers who have an excellent knowledge in hacking. Such profiles may get hacked. Attackers share posts that may deform the company image and cause damage to it. Twitter in KSA contains many fake profiles that may not be detected until the victims announce their profiles in a video or trusted media. The following are examples of the most famous hacked accounts on Twitter and FB in KSA and other places.

An attacker on Twitter impersonated prince Fahad bin Khalid, the head of Saudi Arabian football club Al-Ahli. He published false news about the club boycotting sports channels, which affected the Saudi sports community until confirmed that the person behind the profile is impersonating the prince [34].

Another fake Twitter account appeared impersonating prince Abdulaziz bin Fahad Al Saud, who has a verified profile already with the same image and username, but with one additional letter. The counterfeiter profile appeared in the same style and character of the prince and lured many people to contacting and believing the attacker [35].

The official Twitter profile of prince Sultan bin Salman, head of Saudi commission for Tourism and Antiquities, got hacked by a hacker group called "Cyber of Emotion”. The hacker group published several tweets critical of the tourism sector. The commission affirmed in a statement that the profile was hacked and announced that they welcome the constructive criticism and suggestions from the public. The commission confirmed that they would answer with transparency and clarity all the questions that were published by the hacker group. They were able to recover the profile by help from Twitter technical support [36].

The same hacker group "Cyber of Emotion" was able to hack the official profile of the principality of Al-Madinah in Twitter. They launched an attack on the center of information technology, pointing out that the laws do not have validity and do not apply to reality. In a letter addressed to the principality of Al-Madinah they said "Dear principality of Al-Madinah: The hacked of this profile is not for personal reasons, but because of the lack of attention to the errors sent from us…Cyber of Emotion." They added, "It appears that the hack is unique today, but we wanted to deliver a message that our existence lies not only in the sites, but here as well?”. They concluded: “We apologize for the intrusion of the principality of Al-Madinah, we wish that we will not to be punished for what we did because if it fell in the hands of someone else it will become a bigger scandal…Thank you" [37].

The official profile of the Saudi Ministry of Justice was exposed to breach by an anonymous; in his Tweets he asked some questions and requested answers. The attacker said that he broke into the account because of the ministry’s negligence in information security. He also wondered about the cost of developing the ministry's website [38].

The official Twitter profile of prince Faisal bin Turki, the head of Al-Nassr football club was hacked by a club fan hacker called himself “King Bender”. He tweets using the prince profile to thanking him and congratulating the team for winning the league. The same hacker hacked the official Twitter profile of prince Abdulrahman Bin Mosaad Chief of Al-Hilal Football Club which is considered the rival team of Al-Nassr [39].

PayPal profile on Twitter was under attack by unsatisfied customer who used Twitter platform to complain about their service. A quick announcement came from PayPal to comfort the customers and to ensure that the attack was only on the twitter profile [40].

Burger King’s profile was hacked revealing that the company was bought by McDonalds. Fortunately, the disaster turned into a hilarious and successful advertisement for them, and they gained over 60,000 new followers [40].

Fox news Twitter account got hacked allegedly by Anonymous. Think Magazine interviewed a member of the Scriptkiddies, he said “Fox News was selected because we guessed their security would be just as much of a joke as their reporting." [40].

The Syrian Electronic Army hacked the Guardian’s Twitter profile. They also hacked other major accounts; such as, the Financial Times, BBC News, CBS News and Associated Press [40].

A number of sports celebrities also have fallen victim to their personalities impersonators on FB, including Mohamed Aboutrika, Al-Ahly player. The number of pages that bears his name on FB reached 138 pages. The irony is that Aboutrika does not know anything about these pages, which publishes news about him as if he was the page owner [41].

Ahmed Fathy Al-Ahly and Egypt national team player was surprised by a page bearing his name on FB that was publishing false news about him such as leaving Al-Ahly club and receiving a professionalism from European teams. Fathy said, "I do not have any page on FB or any other website, there are people who pass themselves off as me by using my name and picture. He added: “The number of pages by my name are more than 20 pages and unfortunately, I discovered that a lot of Al-Ahly fans were a victim of those pages and followed them thinking it is my personal page. He concluded: “Many of my friends in the team suffer from the same issues, which caused them a lot of problems because some statements falsely attributed to them on these pages” [41].

It is noteworthy that some of the official governmental profiles had witnessed a penetration by "hackers". Attacks aimed at abusing and sending messages in the wrong and controversial ways.

From all of the above examples, we see that identity theft is a serious problem with severe consequences. Solving this problem requires intensifying the efforts to follow up on the offenders and imposing heavy fines and punishment on them. SN’s are now considered a source of information for celebrity news and official government agencies. Thus, their SN’s profiles must be verified to prevent the spread of rumors and confusion between people.

D. Security Settings In Social Networks

Since SN being used by millions of people as a communication platform, a lot of Information is associated with users' posts such as physical locations, users’ preferences, and social relationships. These sites are the fastest and simplest way to find users’ personal information. In particular, the users of Twitter and FB should be concerned about what personal information they share in their profiles and how others may use it. Thus, before users sign up in SN's, they need to think about how these websites protect them and if they can trust them to share their personal information [42, 43]. The next part is an explanation of security settings in Twitter and FB.

1) Security settings in Twitter

- **Login Verification:** Is off by default. It is so important because it make it harder for an unauthorized person to login to the user account by receiving a confirmation login request via a text message [44, 45].
- **Password Reset:** It is off by default, and it requires user email or phone number to reset his/her password [44].
- **Apps:** A record of all the applications that have access to Twitter account. Users can revoke access for unwanted applications [46].
- **Tweet Location:** It is off by default but when a user is tweeting from his/her phone the default setting is on [47].

2) Security settings in FB

- **Login Notification:** It is off by default. This feature notifies the user by email or text messages if his/her account was accessed from a device they have not used earlier [48].
- **Login Approvals:** It is off by default. It requests from the user to enter a code that was sent to his/her phone when he/she accesses his account from a device that they never used before. After logging in, the user can save this new device into his/her account list of trusted devices [49].
- **Code Generator:** It is part of login approvals, and it is creating a security code every 30 seconds even when users are not connected to the Internet. In addition, the user can use it when resetting his password [50].
- **App Passwords:** It is off by default. A one-time password the user can use to login to his FB App and it helps to keep FB's original password safe [51].
- **Trusted Contacts:** User closest friends who can securely help him if he/she has a problem to access his/her account. For example, when a user forgets his password, and he cannot access his email to reset it [52].
- **Logged-in List:** Shows a list of all user browsers and devices that were used to login to a user's account recently [53].
- **One-time Password:** It is password used when a user is not comfortable to enter his real password. For example, when the user is in a public place [54].

E. Identity Verification Systems in SN's

Fake profiles mostly post misleading information, images and other data that eventually deforms the victim's public image. Therefore, to reduce the possibilities of theft and fraud, appropriate identification systems must be used in order to make sure of the user's identity. Various techniques can be used such as biometric systems e.g. fingerprint and iris recognition. These systems send the biometric data from the input devices to a central processing unit to identify the identity of the users. By using this system, we can guarantee a person's validity and prevent crimes before they occur [55].

The problem emerged in the SN's because we cannot use known identity verification systems; such as, fingerprint and eye print over the Internet. Moreover, it will not be a clever move and unsafe for the users. Therefore, the need for other verification systems became a necessity to make sure of users' identities, and that they are real and not fake.

In SN's, there is a difference between confirmation and verification. Confirmation is a message sent by the site to the user's email or phone to secure the account. For identity confirmation, some sites used phone numbers or emails, and others gather the two methods to ensure greater security for the users. Still the problem of personality verification and the possibility of identity theft exist. While verification is an affirmation from the same site that the owner of this account is the same person who uses it.

Twitter and FB offer two services verification and confirmation. In confirmation, they use two methods to confirm the account by email and phone. However, verification is limited to public figures, celebrities, and governments. Verified accounts are the accounts that have a blue badge with a checkmark, meaning that they are real celebrities or brand profiles and not fake [1, 56].

V. Results and Analysis

We conducted an online survey to study the user's knowledge about the importance of privacy and security in SN's and the extent of user awareness of these issues in the KSA. The purpose of this survey is to evaluate the amount of information that the users typically disclose and what the privacy settings they have applied to protect their profiles. The survey consists of 18 questions with a total of 510 users, representing ten cities "Fig. 1", participated in the survey.

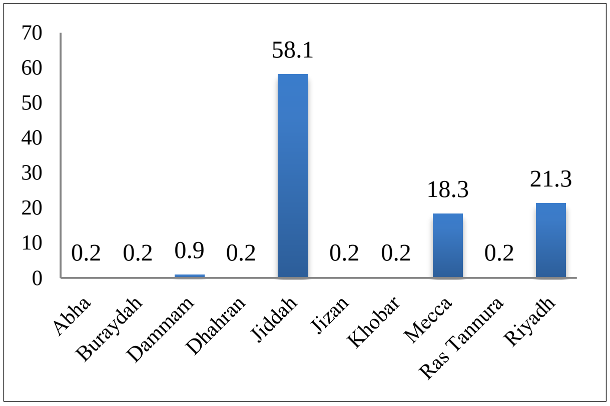

Fig. 1. Survey total responses rank by cities

A. Survey Summary

When analyzing quantitative and qualitative data, the highest response rate (57.1%) was from female participants, where the lowest response rate (42.9%) was from male participants “Fig. 3”.

Most respondents aged between 16-20 years old (23.3%), where least respondents aged between 41-45 years old (4.7%) “Fig. 2”.

For the level of education, "Fig. 4" shows that the most participants were undergraduate users (38.2%) and Twitter was the most popular SN’s among them. The youngest participants were elementary school users (4.9%), and Instagram was the most popular SN’s among this group “Fig. 16”.

(58.6%) Of participants agreed that the benefits of SN’s sites overcomes their risks, therefore (58.3%) of the users want to verify their profiles on SN’s “Fig. 5”.

(6.5%) Of participants does not use SN’s “Fig. 6”, and the reason that prevent (48.5%) of them from signing-up is the social and religious irregularities, especially that there are a lot of inappropriate profiles on SN’s. The second reason is that the SN’s are not safe in terms of privacy (42.4%) “Fig. 7”.

On the other hand, (93.5%) Of all participants sign-up in SN’s. (63.9%) of them selected “to communicate with their friends and families”, and (57.7%) of them selected “finding useful information” “Fig. 8”.

We found that participants prefer to write a partial of their real name on their profiles (45.5%) rather than their real name (32.5%) or a fake name (22.0%) “Fig. 9”.

(43.6%) Of participants choose to make their profiles public to everyone and only (31.7%) prefer to make their profiles private to friends and family “Fig. 10”.

The three prevalent information users like to share are email (64.2%), city (38.4%), and phone number (34.8%) “Fig. 11”.

The result shows that (55.4%) of users only trust the news and information from verified profiles while (26.4%) of users always check the well-known newspapers. In contrast, (18.2%) of users believe any news and information on SN’s “Fig. 12”.

(50.1%) Of participants are confident in their level of privacy, in return (49.9%) of participants are not sure in their level of privacy on SN’s “Fig. 13”.

(75.5%) Of users does not read the privacy policy "Fig. 14" and maybe that is the reason that (78.0%) of them do not trust the SN’s provider in protecting their personal information “Fig. 15”.

B. Discussion

1) People who do not own a SN’s account

33 Of the participants do not have accounts in SN’s; most of them are older than 46 years old. The main reasons for this are they found that this site's overwhelmed with social and religious irregularities and it is not safe in terms of privacy and security. They see the bad side of SN’s where there is a lot of impersonation, rumors and harassment. Some of them find it hard to fully understand it and get used to it. Other simply does not find the time or the interest to be a part of such sites.

We have found that older people do not want to join SN’s because of the negative sides. They consider it an unsafe environment for them. The youngsters do not have fully understood the value and the importance of privacy in order to maintain their personal information. On the contrary, they share every single detail about their personal life on their accounts.

Therefore, it becomes a cause of defaming to them, and it can be used against them in the future. The majority of concerned parents do not want their children to join this community because their children are not aware of the meaning of security policies and related problems, and they are not old enough to make smart decisions. For that, children and many adults need to be given enough knowledge and awareness about to protect their information and how to maintain their privacy.

2) People who do have a SN’s account

The ages of the participants are diverse, were the most interactive group that is involved in SN’s are teenagers and young adults. While 58% of the participants believed that, the benefits of SN’s overcome its risks. Teenagers and young adults were the two groups that thought otherwise “Fig. 17”. The majority of the two groups believed that the risks outweigh the benefits, yet they have active accounts!. The number of female participants outnumbered males by a narrow margin estimated by (14%) this could be evidence that the female users are more than the male users.

The results show that the most used SN’s in KSA respectively are Twitter, Instagram, YouTube, FB, and Google+. The most famous SN’s among elementary and middle school are Instagram. Where for high school, undergraduate and higher education was Twitter “Fig. 16”. As for the benefits of SN’s, the most purposes were to entertain and spend time, Find useful information and of course communicate with friends and family. The teenagers score the highest rate in selecting a fake name or a part of their real name and as the age increased, the participants choose to write their full real names.

The level of privacy was different according to the level of the education. Where the school students and undergraduate were more open in their privacy as they choose their profile to be public. While some of them did not care about their privacy setting or they did not know about it. In return, the higher education participants were more conservative about their privacy were they want their profiles to be private to their friends and families “Fig. 18”.

As a result, the users who made their profiles public were the majority of participants who wanted to verify their profiles. While the users who made their profiles private were the minority of participants who wanted to verify their profiles.

The ranking of information that user share the most on SN’s are email, city, phone number, interests, images, local location, education and marital Status. 15.5% of the participants share nothing on their profiles, and those are the ones who did not care about verifying their profiles as they did not find the need to protect their information.

Teenagers are the most confident in the news and information published in SN's sites. Compared to the rest of the participants where they do not trust any information except for news published by the government verified profiles. However, in many cases, these accounts may be exposed to theft and could release a lot of misleading information before they are restored.

The biggest problem in misunderstanding how SN's deals with the user's information is related to the fact that the users never read the privacy policy. A lot of users don't know how SN's providers protect or deal with their personal information. Therefore, the majority of the participants do not trust SN providers.

C. *The Social Experiment*

1) *Twitter social experiment*

For our first Twitter experiment, we tested the user's knowledge and awareness in security. We sent them a link in the broadcast as follows "To verify your account on twitter quickly just click on the following link.". In the first page, we asked the participant to enter his/her Twitter username. When they did that, we directed them to page number two where we described our experiment to them.

The plan is to see how people's confidence in the anonymous links that asks them to provide private information. Even though we asked them to give something general "their username", but it also shows how much they are willing to give their personal information to anonymous and strangers. 198 (43%) users entered the link; only 55 (28%) users did not enter their usernames "Fig. 19".

143 (72%) users entered their Twitter usernames. The reason behind that from their point of view is they consider usernames public and okay to share. However, this information is considered valuable to a stranger who does not know that the respondent own a Twitter account in the first place. Through this information, he can monitor them, know their information, and even hack their profile or email to gain access to more info.

TABLE I. TWITTER LINK

	Elementary	*Middle School*	*High School*	*Undergraduate*	*Higher Education*
Users who enter the link	14	50	55	55	24
Users who enter the username	9	46	40	35	13
Users who didn't enter the username	5	4	15	20	11

**Check the appendix*

2) *FB and Twitter experiment*

In this experiment, we wanted to prove that penetrating private accounts are very easy. The idea is to select a public profile at random, clone the profile with a similar username, and send friend requests to friends who have private profiles. Of course, if the friend accepted our request we were able to see all of their information. (all the people whom we contacted were sent an apology message and their data was not touched). We did the same experiment on two public accounts, one from FB and the other one from Twitter.

On FB, we chose a public account X for our experiment. Then we created a new account with the same name. In addition, we changed the profile picture and the cover photo to the same real ones. After that, we sent requests to private accounts on X's list. The total requests we sent were 121, and the responses we got were 30, about 24.8%.

On Twitter, we choose a public account Y for our experiment. Then we created a new account with a username Y' (close to the real username), and we changed the profile picture to the same real one. After that, we requested to follow the private accounts. The total requests we sent were 75, and the responses we got were 33, about 44%.

The results from this experiment show us many points:

- Public profiles can be cloned very easily on both networks.
- Public profiles can endanger private ones on their lists.
- Friends of the victims show high acceptance for any incoming messages from their fake friends.
- We noticed that FB provides more settings to protect privacy and security.
- Twitter users are more willing to accept such requests than those of FB.

Of course, we realize that the numbers we got cannot be trusted because of the small sample, however, for ethical reasons, we didn't want to involve more accounts in this experiment; as the goal was just to prove the simplicity of the process.

VI. WAYS TO PROTECT OUR PRIVACY

Based on this research, we would like to emphasize that privacy is a personal responsibility; users should not give their personal information to others who may use it illegally. SN's continually change their privacy policies to protect themselves and to put the blame on the users. According to [57, 58] users can do the following:

- **Secure your PC against theft:** Activate hard disk encryption and always use password to access your devices. Continually update your operating system, security packages and review your web browser security setting. Install and automatically update your anti-virus, anti-spyware software, use an anti-phishing tool and use a good firewall.
- **Be careful when you share your personal data:** Always be careful from sharing your personal information with strangers and trusted people especially over unsecure medium.

- **Do not use one email:** Create a new email for SN's sites and do not use your personal email or work email to sign-up in SN's. Do not share your email that you used to register with anyone and do not choose a username that is similar to your email. If a hacker knows your email, you will facilitate his job to send you viruses or suspicious links. Make sure to use a real email in your profile to help you to restore your forgotten password.
- **Create a difficult password:** Users should not use weak passwords in personal accounts or use the names of relatives as password as that can be easily guessed. Many software systems can identify weak passwords. Moreover, users should not use the same password for all accounts. When creating a new password, use letters, numbers, and symbols at the beginning or end of the password. Users should always try to make the password at least 12 characters to make it unpredictable and impenetrable and never use a password similar to email or username.
- **Be careful with any message from a stranger:** Attackers use different methods and different messages to reach their victims. A careful user will always very the sender before responding to such messages.
- **Be careful of phishing:** Phishing is an attempt to gain sensitive data such as username, password, and credit card information by impersonating trustworthy pages in SN's. Some hacker will pretend to help you in promoting your profile by increases your followers or protecting your account. Where he will ask you to enter your personal data in false sites that look similar to the real one. To protect against phishing attacks, experts advise paying attention not opening a suspicious link and ignoring any request to enter your personal data unless it is the official site otherwise your account will be at risk. Furthermore, make sure access to the company's website via the correct URL.
- **Stay away from Spyware:** Programs and messages reach many users through SN's and email. Some messages contain wrong information aimed at stealing user's data. Users need to ignore messages that they do not know their origin and update antivirus software regularly.
- **Do not download unknown software for portable devices:** Many users download unknown software or games to their devices. Many of such applications can be malware. Users need to be careful when loading any unknown programs; they should only deal with websites of the reliable and well-known companies.
- **Avoid the use of public computers or networks:** Many risks exist when using public devices or network, such as in libraries, cafes and airports, especially when reviewing the financial statements. If necessary, use it but be careful, you must delete personal files, cookies, and Internet history and never forget to log out.
- **Very job posters:** Before sending an application online or in person make sure that the advertiser is a real company.
- **Make your profile "private":** Based on our experiment, users should always choose to have private accounts and be cautious when accepting requesting from friends who have public accounts.

VII. Conclusion and Future Work

There is no doubt that SN's provide a wide range of benefits to users. However, those benefits are not free of risks. Sever risks of privacy breaches and Identity Theft exist. The facts that the majority of users are not aware of such risks and that SN's providers lack proper protection and verification methods make the situation much worse.

In KSA, our survey revealed many results some of which are scary. The fact that 59% of all participants believe that the benefits of SN's outweigh their risks justifies the unprecedented increase in the number of users. When 43% of all profiles are public, and 25% are not aware of their privacy settings, the privacy of those with private profiles is at a great risk. Other results show that the majority never read privacy policies, share too much information, and have confidence in SN's.

Our small experiment revealed that users with private accounts are not safe as well. Having friends with public profiles endangers the privacy of such users.

To improve the privacy of users and reduce their risks we provided a list of recommendations. We believe that awareness at a national level is needed, users need to be cautious and protective, and SN providers need to provide more protection and verification to users.

Finally, from the experiment's results we found that Facebook provides more privacy and security tools than Twitter. Therefore, identity theft cases on Facebook appear to be less than that of Twitter.

References

[1] Facebook, (2014). Facebook Website. [online] Available at: http://www.Facebook.com [Accessed 12 Sep. 2014].

[2] K. Finklea, 'Identity Theft: Trends and Issues', Congressional Research Service, 2014.

[3] S. Gazette, 'Use of mobiles in social media on the rise in KSA', Saudigazette.com.sa, 2014. [Online]. Available: http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20140109192016. [Accessed: 17- Apr- 2014].

[4] S. Al-Qahtani, 'hackers loot 2.5 billion SR from 3.5 million Saudi in one year', Alsharq.net.sa, 2013. [Online]. Available: http://www.alsharq.net.sa/lite-post?id=792821. [Accessed: 24- Nov-2013].

[5] Citc.gov.sa, 'Anti-Cyber Crime Law', 2007. [Online]. Available: http://www.citc.gov.sa/English/rulesandsystems/citcsyste/pages/cybercrimesact.aspx. [Accessed: 17- Nov- 2014].

[6] Reznik, Maksim (2013) "Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation," Touro Law Review: Vol. 29: No. 2, Article 12.

[7] K. Krombholz, D. Merkl and E. Weippl, 'Fake identities in social media: A case study on the sustainability of the Facebook business model', Journal of Service Science Research, vol. 4, no. 2, 2012.

[8] Stutzman, Fred and Kramer-Duffield, Jacob (2010): Friends only: examining a privacy-enhancing behavior in Facebook. In: Proceedings of ACM CHI 2010 Conference on Human Factors in Computing Systems 2010. pp. 1553-1562.

[9] Verma, D. Kshirsagar and S. Khan, 'Privacy and Security: Online Social Networking', Association of Computer Communication Education for National Triumph (ACCENT), vol. 3, no. 8, pp. 310-315, 2013.

[10] L. Bilge, T. Strufe, D. Balzarotti and E. Kirda, 'All your contacts are belong to us: automated identity theft attacks on social networks', pp. 551--560, 2009.

[11] M. Al-Mujeb. "Saudis' Awareness of Privacy Risks on Facebook" M.A. thesis, University of Glamorgan, UK, 2010.

[12] R. Demyati. "Privacy Issues in Facebook" M.A. thesis, Australia, 2011.

[13] Catherine D. Marcum, George E. Higgins (April 28, 2014 by CRC Press) Social Networking as a Criminal Enterprise. Criminal Justice & Law [Online]. Available at: http://www.crcpress.com/product/isbn/9781466589797 (Accessed: 31 Nov 2014).

[14] Joy Mali (2012) Identity Theft Through Social Networking, Available at: http://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html (Accessed: 14 Nov 2014).

[15] Bernard Pragides, Identity Theft and Social Networking Sites, Available at: http://www.streetdirectory.com/travel_guide/140727/identity_theft/identity_theft_and_social_networking_sites.html (Accessed: 14 Nov 2014).

[16] T. Clinic Team, 'The State of Social Media in Saudi Arabia 2012', The Social Clinic, 2013. [Online]. Available: http://www.thesocialclinic.com/the-state-of-social-media-in-saudi-arabia-2012-2/. [Accessed: 08- May- 2014].

[17] T. Clinic Team, 'The State of Social Media in Saudi Arabia 2013', The Social Clinic, 2014. [Online]. Available: http://www.thesocialclinic.com/the-state-of-social-media-in-saudi-arabia-2013/. [Accessed: 08- May- 2014].

[18] Smith, 'Why Americans use social media', Pew Research Center's Internet & American Life Project, 2011. [Online]. Available: http://www.pewinternet.org/2011/11/15/why-americans-use-social-media/#fn-250-1. [Accessed: 14- Jun- 2014].

[19] Mbrsg.ae, 'Arab Social Media Outlook 2014', 2014. [Online]. Available: http://www.mbrsg.ae/HOME/PUBLICATIONS/White-Papers-(1)/Arab-Social-Media-Outlook-2014.aspx?lang=en-US. [Accessed: 23- Oct- 2014].

[20] S. HIMELFARB and S. ADAY, 'Media That Moves Millions', Foreign Policy, 2014. [Online]. Available: http://www.foreignpolicy.com/articles/2014/01/17/media_moves_millions_social_ukraine_twitter. [Accessed: 07- Nov- 2014].

[21] M. Habash, 'How does Facebook achieve its profits?', Tech-wd, 2012. [Online]. Available: http://www.tech-wd.com/wd/2012/05/28/how-can-facebook-make-money/. [Accessed: 28- Oct- 2014].

[22] Facebook.com, 'Under the Hood: The Entities Graph', 2014. [Online]. Available: https://www.facebook.com/notes/facebook-engineering/under-the-hood-the-entities-graph/10151490531588920. [Accessed: 13- Nov- 2014].

[23] Carrns, 'Careless Social Media Use May Raise Risk of Identity Fraud', Bucks Blog, 2012. [Online]. Available: http://bucks.blogs.nytimes.com/2012/02/29/careless-social-media-use-may-raise-risk-of-identity-fraud/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1. [Accessed: 14- May- 2014].

[24] INVISUS (2014) How Identity Theft Happens, Available at: http://www.idefendfamily.com/how_id_theft_happens.aspx#cs (Accessed: 15 Nov 2014).

[25] Gunatilaka, A Survey of Privacy and Security Issues in Social Networks, 1st ed. 2011.

[26] Carnegie Mellon University (2014) How cyber criminals operate, Available at: http://www.carnegiecyberacademy.com/facultyPages/cyberCrime.html (Accessed: 15 Nov 2014).

[27] P. DWYER, CYBER CRIME IN THE MIDDLE EAST, 1st ed. 2010.

[28] RIVA RICHMOND (May 2, 2010) 'Stolen Facebook Accounts for Sale', The New York Times, pp. B3 [Online]. Available at: http://www.nytimes.com/2010/05/03/technology/internet/03facebook.html?_r=0 (Accessed: 15 Nov 2014).

[29] Hayley Dixon (2013) 'Online dating sites use stolen data to create fake profiles, it is alleged', The Telegraph, 29 Jul , p. http://www.telegraph.co.uk/news/uknews/law-and-order/10207712/Online-dating-sites-use-stolen-data-to-create-fake-profiles-it-is-alleged.html.

[30] 2012 NORTON CYBERCRIME REPORT, 1st ed. 2012.

[31] Citc.gov.sa, 'Cybercrime Awareness Campaign', 2014. [Online]. Available: http://citc.gov.sa/arabic/MediaCenter/awarenesscampaigns/Pages/PR_AWR_005.aspx. [Accessed: 08- Oct- 2014].

[32] Cert.gov.sa, 'Computer Emergency Response Team - SA', 2014. [Online]. Available: http://www.cert.gov.sa/index.php?option=com_frontpage&Itemid=1. [Accessed: 07- Oct- 2014].

[33] Internet.sa, 'Reporting on impersonation (Twitter) | Internet Saudia Arabia', Web1.internet.sa. [Online]. Available: http://web1.internet.sa/ar/twitter_impersonate/. [Accessed: 08- Oct- 2014].

[34] Alarabiya.net, 'Hacker penetrates the head of Al-Ahli club account in Twitter', 2014. [Online]. Available: http://www.alarabiya.net/articles/2012/04/15/207846.html. [Accessed: 10- Nov- 2014].

[35] H. Lhd, 'User impersonating Prince Abdulaziz bin Fahd on Twitter', Burnews.com, 2014. [Online]. Available: http://www.burnews.com/news/2012/03/31/مغرد-ينتحل-شخصية-الامير-عبد-العزيز-بن-فهد-على-التويتر. [Accessed: 14- Nov- 2014].

[36] M. Houdad, '"Tourism" undertakes to answer the questions from the hacker', Sabq.org, 2014. [Online]. Available: http://sabq.org/kvngde. [Accessed: 14- Nov- 2014].

[37] K. Ashamany, '"Hacker" penetrates the profile of principality of Al-Madinah in "Twitter"', Sabq.org, 2014. [Online]. Available: http://sabq.org/Ijngde. [Accessed: 17- Nov- 2014].

[38] Y. Al-Otaibi, '"Hacker" penetrates Ministry of Justice account in "Twitter"', Sabq.org, 2014. [Online]. Available: http://sabq.org/W1ngde. [Accessed: 17- Nov- 2014].

[39] Barqawi, 'For thanking and challenging', Sabq.org, 2014. [Online]. Available: http://sabq.org/u7Xfde. [Accessed: 17- Nov- 2014].

[40] J. Philips, '7 Examples of What Happens When Your Twitter Account is Hacked - Jeffbullas's Blog', Jeffbullas's Blog, 2013. [Online]. Available: http://www.jeffbullas.com/2013/07/12/7-examples-of-what-happens-when-your-twitter-account-is-hacked/. [Accessed: 03- Oct- 2014].

[41] H. Zayed, 'Impersonation on "Facebook"', Alwatan.com.sa, 2014. [Online]. Available: http://www.alwatan.com.sa/Nation/News_Detail.aspx?ArticleID=76105. [Accessed: 17- Nov- 2014].

[42] Beach, M. Gartrell and R. Han, 'Solutions to security and privacy issues in mobile social networking', vol. 4, pp. 1036--1042, 2009.

[43] Securityinabox.org, 'How to Change Basic Account Settings on Twitter | Security In A Box', 2014. [Online]. Available: https://securityinabox.org/twitter_basic#2.1. [Accessed: 20- Sep- 2014].

[44] L. Hardwick, 'How to improve your Twitter security and privacy', Naked Security, 2014. [Online]. Available: http://nakedsecurity.sophos.com/2014/08/26/how-to-improve-your-twitter-security-and-privacy/. [Accessed: 26- Sep- 2014].

[45] Support.twitter.com, 'Twitter Help Center | Using login verification', 2014. [Online]. Available: https://support.twitter.com/articles/20170388. [Accessed: 24- Sep- 2014].

[46] Support.twitter.com, 'Twitter Help Center | Connecting or revoking third-party applications'. [Online]. Available: https://support.twitter.com/groups/57-safety-security/topics/276-understand-your-settings/articles/76052-connecting-or-revoking-third-party-applications. [Accessed: 08- Oct- 2014].

[47] Support.twitter.com, 'Twitter Help Center | Adding your location to a Tweet'. [Online]. Available: https://support.twitter.com/groups/57-

safety-security/topics/276-understand-your-settings/articles/122236-adding-your- location-to-a-tweet. [Accessed: 08- Oct- 2014].

[48] Facebook.com, 'What are login notifications? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/162968940433354. [Accessed: 08- Oct-2014].

[49] Facebook.com, 'What are login approvals? How do I turn this setting on? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/148233965247823. [Accessed: 26- Sep-2014].

[50] Facebook.com, 'What is Code Generator? How does it work? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/270942386330392. [Accessed: 27- Sep-2014].

[51] Facebook.com, 'How do I use app passwords? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/249378535085386/. [Accessed: 28-Sep- 2014].

[52] Facebook.com, 'What are trusted contacts? How do I add trusted contacts to my account? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/119897751441086. [Accessed: 28- Sep- 2014].

[53] Facebook.com, 'How can I manage where I'm logged into Facebook? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/174571515935086. [Accessed: 08- Oct-2014].

[54] Facebook.com, 'What's a one-time password and how do I get one? | Facebook Help Center | Facebook'. [Online]. Available: https://www.facebook.com/help/214309978590084. [Accessed: 08- Oct-2014].

[55] Identity Verification and Social Information, 1st ed. Trulioo Information Services Inc.

[56] Twitter.com, 'Welcome to Twitter'. [Online]. Available: http://www.twitter.com. [Accessed: 08- May- 2014].

[57] Rami, 'How to protect yourself from identity theft online', Alwakei.com, 2012. [Online]. Available: http://www.alwakei.com/news/19894/index.html. [Accessed: 02- Apr-2014].

[58] K. Williams, A. Boyd, S. Densten, R. Chin, D. Diamond and C. Morgenthaler, 'Social Networking Privacy Behaviors and Risks', Seidenberg School of CSIS, Pace University, USA, 2009.

[59] M. Whitman and H. Mattord, Principles of information security, 1st ed. Boston, Mass.: Thomson Course Technology, 2003.

APPENDIX

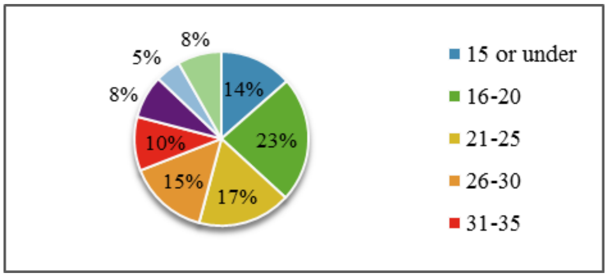

Fig. 2. Participants ages

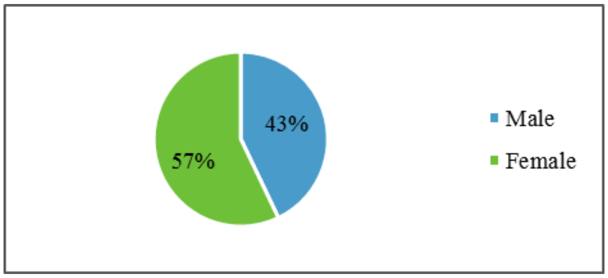

Fig. 3. Participants gender

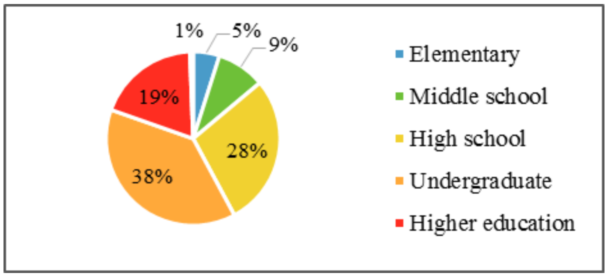

Fig. 4. Participants level of education

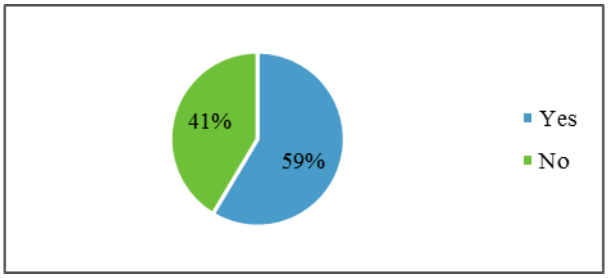

Fig. 5. Does the benefits of SN's overcomes the risks

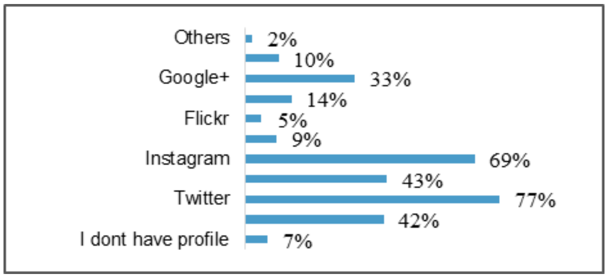

Fig. 6. Participants Profiles in SN's

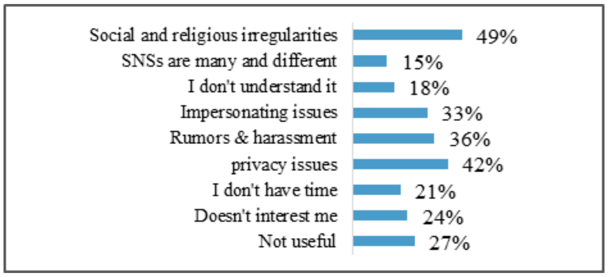

Fig. 7. Reasons that prevent users from participating in SN's

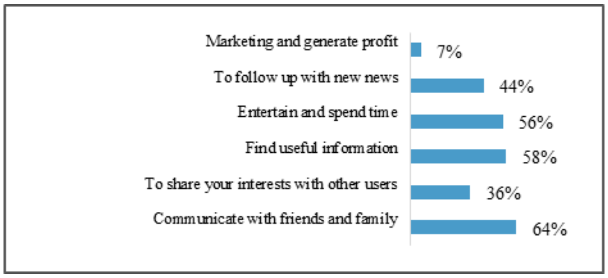

Fig. 8. Reasons participants use SN's

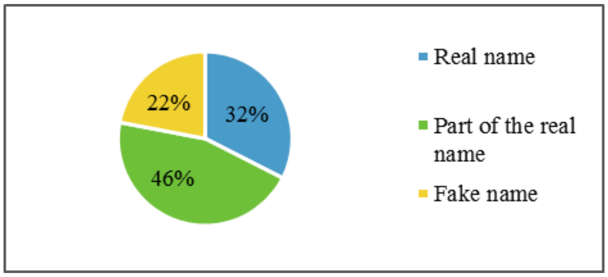

Fig. 9. User's name on SN's

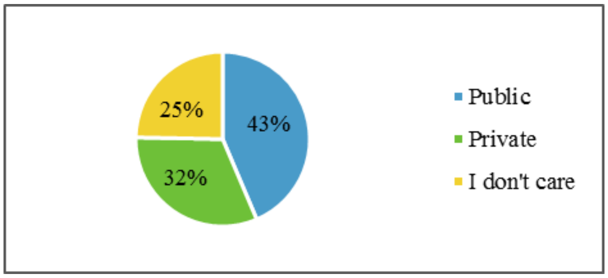

Fig. 10. The level of privacy

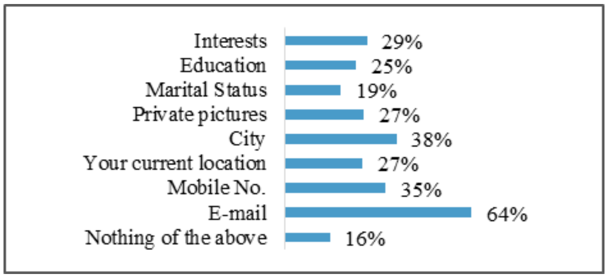

Fig. 11. Information users share on SN's

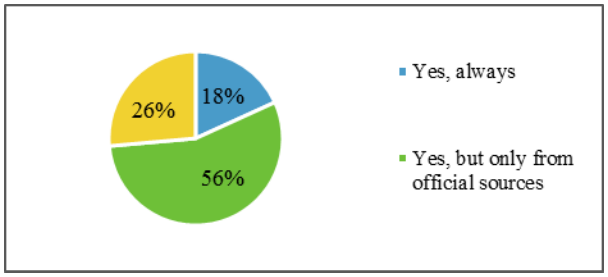

Fig. 12. Users confidence in news on SN's

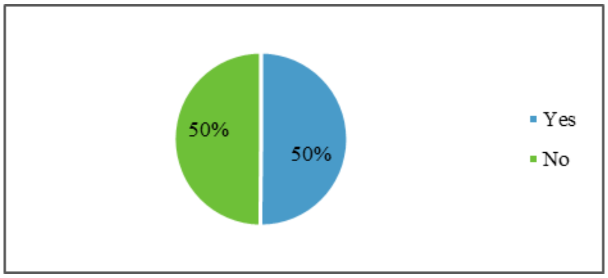

Fig. 13. User's confidence in their level of privacy

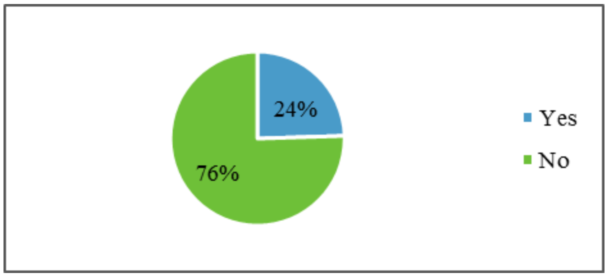

Fig. 14. Do you read the privacy policy

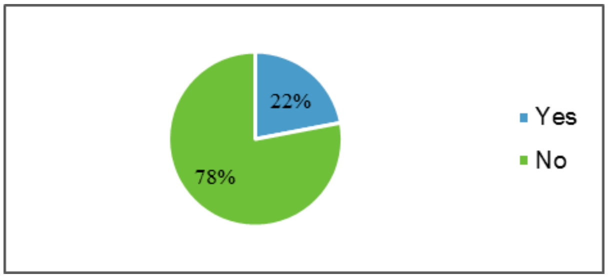

Fig. 15. Users confidence in SN's providers

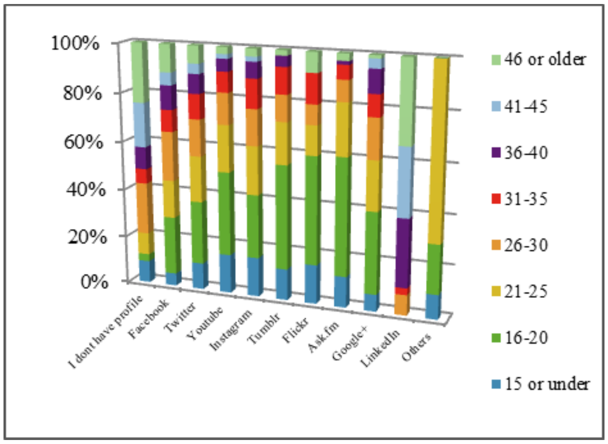

Fig. 16. Relation between users ages and most used SN's

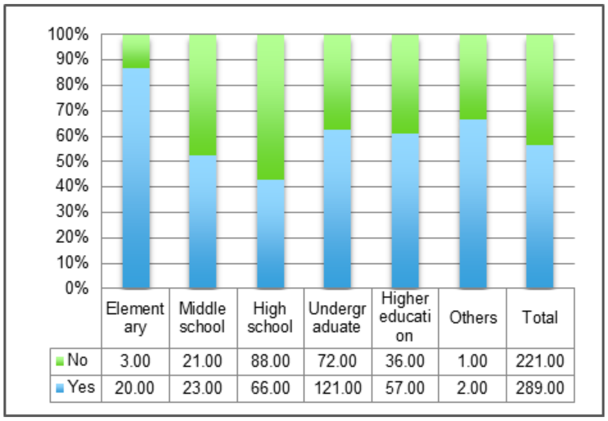

Fig. 17. Relation between users' level of education and benefits overcomes the risks

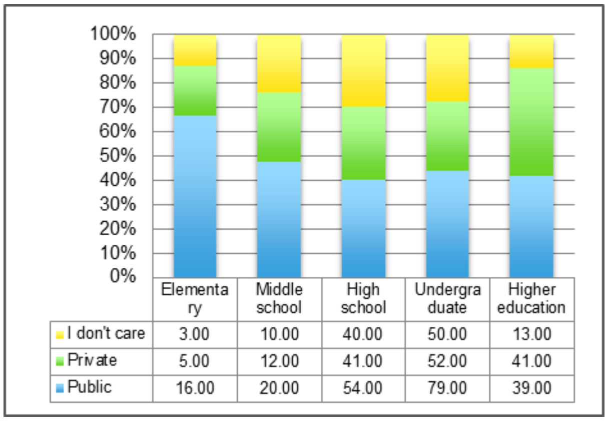

Fig. 18. Relation between users education and level of their profiles privacy

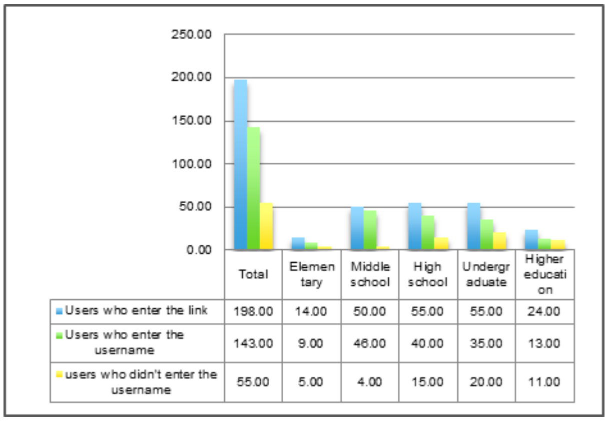

Fig. 19. First Twitter experiments

TABLE II. FBAND TWITTER EXPERIMENTS

Required Information to Sing-up		
	Facebook	**Twitter**
First Name	√	√
Family Name	√	√
Email Address	√	√
Date of Breath	√	X
Gender	√	X
Phone Number	Not required at first but later when the user sign-in he/she must enter a phone number to confirm the account.	√
Confirmation Message	In order to complete the registration FB send a confirmation message to the user email.	In order to complete the registration Twitter send a PIN to the user phone.
Privacy and Security		
Facebook and Twitter provide a lot of privacy options to protect user security where the user can customize it as needed.		
Experiment Results		
Number of Friend Requests Sent By Us	The total requests we sent are 121, and the total responses we get are 30.	The total requests we sent are 75, and the total responses we get are 33.
Percentage	24.8%	44%
The results of the experiment confirmed that Facebook provides more options for privacy and security than Twitter. Therefore, identity theft cases on Facebook appears to be less than that on Twitter.		