2016

Who Stole Me? Identity Theft on Social Media in the UAE

Zeenath Reza Khan
University of Wollongong, zeenath@uow.edu.au

Salma Rakhman
University of Wollongong Dubai

Arohi Bangera
University of Wollongong Dubai

Publication Details

Khan, Z. Reza., Rakhman, S. & Bangera, A. 2016, 'Who Stole Me? Identity Theft on Social Media in the UAE', 4th Global Conference on Business and Social Sciences, Global Academy of Training and Research, Dubai, UAE,

Who Stole Me?
Identity Theft on Social Media in the UAE

Zeenath Reza Khan[1*], Salma Rakhman[2], Arohi Bangera[3]

[1]University of Wollongong in Dubai, P.O Box: 20183, Dubai, UAE
Email: zeenathkhan@uowdubai.ac.ae
[2]University of Wollongong in Dubai, P.O Box: 20183, Email: salma.rakhman@rocketmail.com
[3]University of Wollongong in Dubai, P.O Box: 20183, Email: arohibangera14@gmail.com

ABSTRACT

This paper is a first attempt at investigating the self-reported number of instances of identity theft on social media among student population the U.A.E while providing an overview of its impact.

The Internet provides users with multiple ways to describe and showcase their personalities (Suler, 2002, pp. 455-460 as qtd. in Moise, 2015, p. 118). With the introduction of social networking sites, the number of users is exponentially increasing. Facebook and Twitter have between them about 82% Internet users, an astounding total of 1.2 billion users (Shen, 2013, as qtd. in Zeadally & Tsikerdekis, 2015). Research further suggests that due to the speed at which social networking sites are flourishing, it has become a lot easier to steal content and conduct identity manipulation. Among users, it is posited that students and young adults are the most vulnerable and easy victims of identity theft on social media.

In late 2015, UAE users lost more than five billion dirhams due to cybercrimes such as identity theft (Sophia, 2015). However, little or no research has been conducted on the issue of identity theft on social media to begin to understand the depth of the problem.

As a pilot, this study uses arithmetic analysis to record the first-such study of instances of identity theft among students and its impact on the respondents.

Type of Paper: Empirical

Keywords: Cyberbullying; Facebook; Identity Theft; Social Media; Social Network

1. Introduction

Identity theft is the theft of identity information such as name, personal details and more. As the growth of social media users increases, so does the rate of identity theft (Hoar, 2001). Identity theft has many forms such as insurance identity theft, criminal identity theft, driver's license identity theft and the latest identity theft of social network profiles (Stroup, 2014).

In late 2015, UAE users lost more than five billion dirhams due to cybercrimes such as identity theft (Sophia, 2015). About 17.6 million people in USA were hit by identity theft in 2014, estimating a $15 billion loss for the country (Chaitin, 2014). 770,000 Australian citizens became victims of identity theft in 2015, costing them $15 billion annually (Edwards, 2015). Identity theft doesn't just cause financial loss. Implications range from emotional, psychological and social loss of at least 30 hours on average dealing with consequences (Harrell, 2015).

Researchers have posited that the sudden spike in identity theft in recent years can be attributed to the increase in social media usage. Although social media has facilitated increase and ease of communication, it seems to have also made user's personal information vulnerable and susceptible to identity theft (Lewis, 2016). Globally, the main target of identity thieves seems to be youngsters, aged 15 – 33, commonly known as millennials (Sophia, 2015).

With years of research, statistical surveys and news coverage on the issue of social media identity theft among youngsters, its implications, and possible best practices tailored to countries such as USA, UK and Australia, they have established laws and policies over the years to counter identity theft (Federal Trade Commission, 1998; Australian Law Reform Commission; 1999).

In comparison, the UAE, a fairly young, developing nation, has only just begun to look into the issue. In 2012 a Federal Law called Cyber Crime Law was developed that deals with cyber-crime, but not specifically identity theft through social media (O'Connell & Siassios, 2013).

Conversationally, it is also crucial to understand that while in the USA, the birth place of Internet and social media (Liu, 2014), has about 73% of social media users to date (Statista, 2015), UK recorded a high rate of 53.5% social media users in 2015 (eMarketer, 2015) while Australia had 68% active users on social media in the same year (Ravensdale, 2015). UAE, that celebrated its 44th National Day in 2015, already has 56% social media usage (GMI, 2015). Consequently, despite the severity of the crime and the need for understanding the actual problem on the ground, very little, if any research has been conducted in the country on the actual number of social media identity theft cases among youngsters.

This research surveys school and university students and young adults across Dubai and Sharjah to build a database of cases, record number of instances of such crimes and identify common effects of identity theft in the country. It is believed that conducting such a research can pave the way for better understanding of this problem that plagues youngsters and can help provide possible solutions to parents, schools and community.

2. Information, Communication Technology and Identity Theft

Identity theft is when a person deceitfully acquires and utilizes someone else's character (Gercke, 2007, p. 4, as qtd. in Moise, 2015, p. 120). Hoar (2001) highlights identity theft as a crime advocated by the generation of today. There are various types of identity thefts that can take place in someone's day to day life, ranging from financial identity theft which happens with bank accounts and financial information of a person to insurance identity theft, medical identity theft, criminal identity theft and so many others (Stroup, 2014). According to Siciliano (2011), identity theft can take other forms such as 'new account fraud' wherein the victim's personal information can be used to obtain products and services. This is also similar to the 'account takeover fraud', where in the personal account numbers of the victim is used instead. Identity theft or fraud is estimated to take place every two seconds (Ellis, 2014). In 2013 alone, the number of fraud victims jumped to 13.1 million people, which is very alarming (Ellis, 2014).

2.1 Why is it on the rise?

Research has posited many reasons to why identity theft (IDT) is on the rise. Among these reasons are individual's carelessness, technology advancement, moral disengagement of employees, fraud and abuse techniques, etc. (IT -Analysis, 2003).

Individual carelessness in disposal of personal information provides an opportunity to avail information easily. In the USA, it is forecasted that nearly 70% of IDT came about from disposed information in trash (IT-Analysis, 2003).

Technological advancement corresponds to easier way of committing identity theft. All sorts of computer related fraud such as spamming, phishing, and spyware enables easy IDT actions. For instance, spam emails are composed in an emotional manner highlighting benefits to potential targets, and in return, availing information such as Social Security Number, bank account details, etc. (U.S Department of Justice, 2016).

2.2 Social Media and IDT (SMIDT)

Reznik (2013) demonstrates how social media - an essential part of daily interaction in our society - contributes as an easy method of identity theft. Internet impersonation has flourished due to tremendous growth of social media sites. There exist two methods to execute IDT on social media (SMIDT):

- Creating a fictitious profile of victim and successfully using the identity to communicate and do activities online.
- Either directly or indirectly stealing victim's password, then accessing account to carry out activities.

(Reznik, 2013)

3. Children and SMIDT

A study by Doug and Marje (2009) explains the association of children and SMIDT. Frequent access to technology, irresistible to connect with peers and socializing are factors that motivate children to use Facebook (Doug and Marje, 2009). The extensive use has led to one serious issue among children, which is lack of privacy. Children are naïve, they often misunderstand the sense of privacy and social responsibility; examples include humiliating text, photos, video, hurtful comment and increasing friends and online relations which ultimately results in children being victim of identity theft (UNICEF, 2012).

4. Impact of SMIDT

The Canadian Fraud Prevention Forum (OECD, 2009) pointed out that IDT impacts all types of victims regardless of their age or income level. The United Kingdom loses £670 million and higher because of SMIDT and online fraud due to which the economic positioning of the country suffers majorly (Jones, 2014).

Get Safe Online Week, a campaign coined to raise awareness about SMIDT, conducted a survey with a sample size of 2,075 people, the findings of the survey noted that almost half or 45% of those surveyed had been a victim of SMIDT and other platforms. These victims who felt prey, shared that the experience shocked them to such an extent that they have changed their social behavior completely, now onwards being more alert and vigilant (Jones, 2014).

There is a psychological impact that also exists due to IDT. 40% of the victims experience stress and frustration, 45% experience feelings of mistrust and denial, 85% of the victims feel infuriated with the situation they are in, 42% of the victims find it very difficult to trust anyone after being robbed of their identity on social platforms (The Aftermath Study, qtd. in Guardchild, n.d)

5. SMIDT in the UAE

Of all types of IDT, the credit card theft is very common among the people of the UAE (Maceda, 2011). In September 2015, a Filipino resident of the United Arab Emirates (UAE) was left in a shock when she got to know that there was an active account in a local bank on her name, which she never opened with a cash loan left to be paid for AED 10,130/- (Leon, 2015).

Regardless of common credit card theft, reports in local newspapers have stated that 41% of UAE social media users face suspicious message from cybercrime sorts. Moreover, the reason that lies behind is that 26% UAE respondents use public Wi-Fi while they enter personal data (Bedirian, 2014).

In 2015 the consumers in UAE lost more than 5 billion dirhams due to cybercrimes which included SMIDT and in general (Sophia, 2015). Furthermore, Sophia points out that on an average each person in the U.A.E loses AED 2,331 due to activities caused by cybercrimes, which included SMIDT (2015).

Abu Dhabi police reported 235 cybercrimes in 2010 but ineffective law did not prosecute in maximum cases. As such new defense has been established enhancing the framework of cybercrime law in order to reduce two major online threats which are political activists using social media and governmental institutions getting cyber-attack. Additionally, 2006 law on identity theft was also improved (Anon, 2012).

6. Research Objective

Literature posits that children, particularly aged 12 – 19 are most vulnerable to SMIDT due to their extensive use of social media (Collins 2006; Collins & Hoffman, 2004). However, in the UAE, few if any studies have been conducted in the past to record the instances and the impact of SMIDT among the children in this age group. This paper aims to record instances of SMIDT among students in the nation, and identify some common impacts on students.

7. Methodology

In order to carry out this study, the methodology was as follows:

- A survey tool was developed using DeMaio and Beck (2008) suggestions on possible items to include and Betz (2012)
- Sample population size of 200 were targeted, 128 responded back with appropriate consent
- Items ensured no identifying information was collected, so demographic section only collected information on 'age' and grade/university level
- Second section collected information on respondent's activity on social media including 'number of active accounts', 'number of visits on social media', 'number of friends', etc.
- Third section captured instances of identity theft
- Fourth section captured respondent's feedback on impact of IDT on a Likert Scale

8. Results and Analysis

128 students responded to the questionnaire. As shown in figure below, majority of the respondents were above 18 and enrolled in local universities.

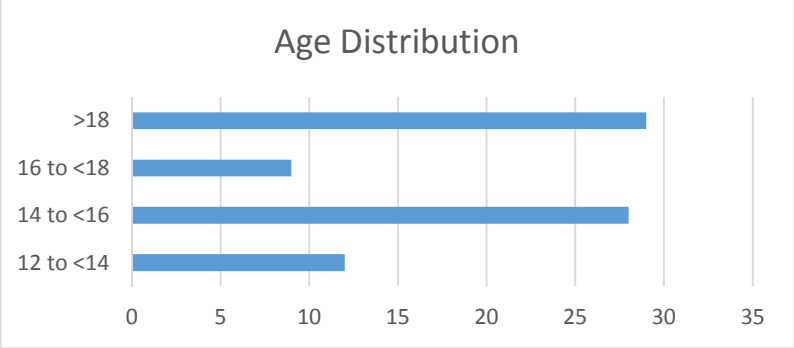

Figure 1: Respondent's Grade Distribution

- 100% of the respondents reported being active users of social media sites.
- Average number of visits to the sites was 16 times per day
- Average number of active accounts was 2 per respondent
- Average number of friends on social media was 70

Overall, the number of instances of SMIDT reported by the responses was only about 59%, as shown below:

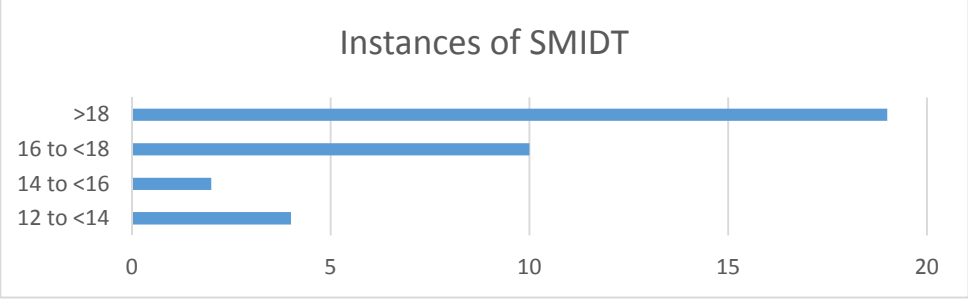

Figure 2: Instances of SMIDT reported by respondents

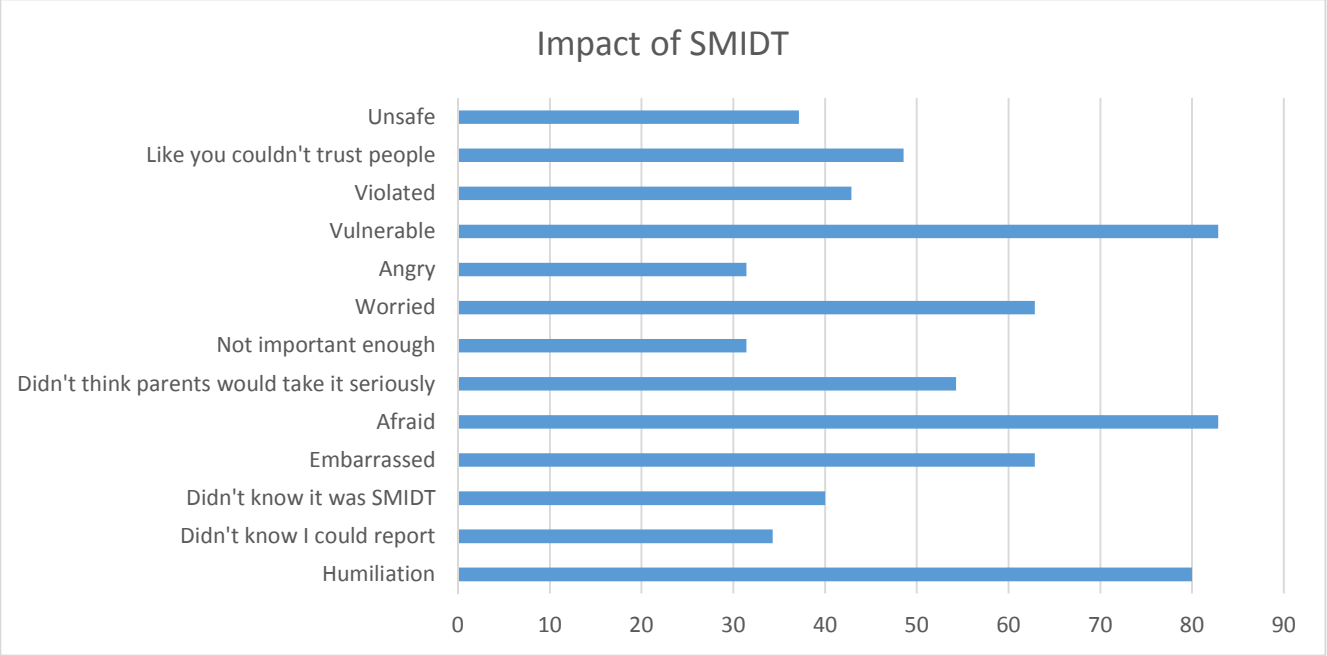

Figure 3: Impact as reported by respondents on a Likert Scale

80% of the respondents strongly felt 'Humiliation' and 'Afraid' due to SMIDT. 63% felt 'embarrassed' and 'worried', 48% felt 'like they couldn't trust people', 42% felt 'violated'.

9. Discussion and Conclusion

The results of this study showed that students between the ages of 12 and 18+ are highly active on social media. Although only 59% of the sample reported being victims of some form of SMIDT, in a small sample size of 128, 59% is considered quite high. This demonstrates that the instances of SMIDT are high among student victims, particularly in the age bracket above 18. Furthermore, the impact of SMIDT on the student victims reported were quite grave from humiliation to trust issues to feeling violated.

There is a psychological impact that also exists due to IDT. According to a study presented in Guardchild, victims experienced stress and frustration, feelings of mistrust and denial, infuriated with the situation they were in, and found it very difficult to trust anyone after being robbed of their identity on social platforms (The Aftermath Study, qtd. in Guardchild, n.d). All of these impacts were mirrored in this study as mentioned above, making the findings valid and relevant.

Aımeur and Schonfeld (2011) remarked that youth are usually victims of identity theft on social media considering the fact that they are not cautious about the kind of information they post on social networking sites and because young people are on social sites way more than the general population. This study has supported this finding and highlighted a 59% rate of victims in a small, controlled study.

Furthermore, as highlighted in previous sections, research has posited that victims of SMIDT are left with permanent wounds and the constant lingering of an irreversible experience. These instances have a long-term bearing on the trust a victim can put in a person or anything for that matter (Marron, 2007). The pilot study definitely supports this finding, where the highest ratings that respondents selected highlight they strongly felt humiliation, could not trust people and didn't think parents would take them seriously.

Sharp et. al (2004) have stated that victims of SMIDT go through states of irritation, anger and physical signs of depression and anxiety. This study also supports this finding. As mentioned above, respondents strongly felt humiliation, embarrassed, angry, worried and vulnerable, violated and not important enough, all of which can have serious implications for the respondents' character and development process.

Though a small, experimental study, the results highlight the significance of such a study in the region, as it brings to light existence of such crimes in the nation. With 59% of the respondents agreeing to have been a victim of some form of SMIDT, this study has highlighted the need for further large-scale study into this matter to collate more data on a larger sample size. Furthermore, with the impacts highlighted, the study sheds light on the seriousness of how the victims feel and is affected by SMIDT, thus making it imperative to bring more notice to the topic to carry out more in-depth studies in the nation.

10. Limitations and Future Study

The study had a few limitations. There is not much information available about SMIDT in the UAE. This posed a problem in reviewing existing literature to justify such a study in the nation. Furthermore, students and their parents were hesitant to give consent to becoming a part of the study to begin with, making the sample size small. Other limitations included the scope of the study itself. It is felt that it was required to first capture respondents' perception and knowledge of SMIDT before recording instances of being victims of the crime.

It is strongly believed that this study has paved the way for a large-scale future study on SMIDT in the UAE that specially targets student population, gathering more data to support the findings of this study which will ultimately help develop tools and techniques to increase awareness of such crimes in order to word towards reducing such crimes and protecting the students form predators.

References

1. Aımeur, E. and Schonfeld. D (2011), 'The Ultimate Invasion of Privacy: Identity Theft', in the Ninth Annual International Conference on Privacy, Security and Trust (PST), IEEE, Montreal QC, 19- 21 July, viewed on 1 April 2016, <http://ieeexplore.ieee.org.ezproxy.uow.edu.au/xpl/articleDetails.jsp?arnumber=5971959>
2. Anon., (2012). Internet- Law & legislation. MEED: Middle East Economic Digest, 56(46), pp. 7-7.
3. Australian Law Reform Commission 1999, 'Criminalizing identity theft', accessed on 15 February 2016, <http://www.alrc.gov.au/publications/12.%20Identity%20Theft/criminalising-identity-theft>
4. Bedirian, R (2014), 'Social media posts fraught with risks', Gulf News, viewed on 22 march 2016, < http://gulfnews.com/news/uae/general/social-media-posts-fraught-with-risks-1.1388581 >
5. Betz, A (2012), "The Experiences of Adult/Child Identity Theft Victims", Graduate thesis and dissertations paper, Iowa State University, viewed on 2 April 2016, < http://lib.dr.iastate.edu/cgi/viewcontent.cgi?article=3764&context=etd>
6. Chaitin, D. (2014). 17.4 million Americans hit by identity theft in 2014. Washington Examiner. Available URL: http://www.washingtonexaminer.com/17.4-million-americans-hit-by-identity-theft-in-2014/article/2572908#!
7. Collins, J. M. (2006). Investigating identity theft: A guide for business, law enforcement, and victims. Hoboken, N.J.: John Wiley & Sons.
8. Collins, J. M., and Hoffman, S. K. (2004). Identity theft victims' assistance guide: The process of healing. Flushing, NY: Looseleaf Law Publications.
9. DeMaio, T, and Beck, J (2008), "Developing Questionnaire Items to Measure Identity Theft", American Association for Public Opinion Research, viewed on 2nd April 2016, < www.amstat.org/sections/srms/proceedings/y2008/files/demaio.pdf>
10. Doug, F. and Marje, M., (2009). Teacher Librarian. the impact of facebook on our students , 36(5), pp. 36-40.
11. Edwards, M 2015, 'Identity theft: More than 770,000 Australians victims in past year', NewsABC, accessed on 15 February 2016, < http://www.abc.net.au/news/2015-04-14/identity-theft-hits-australians-veda/6390570>

12. Ellis, B (2014), 'Identity fraud hits new victim every two seconds', CNN Money, viewed on 21 March 2016, <http://money.cnn.com/2014/02/06/pf/identity-fraud/>

13. eMarketer 2015, 'Young Mobile Users Drive UK Social Media Usage', accessed on 15 February 2016, <http://www.emarketer.com/Article/Young-Mobile-Users-Drive-UK-Social-Media-Usage/1013163>

14. Federal Trade Commission 1998, 'Identity Theft and Assumption Deterrence Act', accessed on 15 February 2016, <https://www.ftc.gov/node/119459>

15. GMI Blogger 2015, 'UAE Internet Social & Mobile Statistics 2015 Infographics', accessed on 15 February 2016, <http://www.globalmediainsight.com/blog/uae-internet-stats-infographics-2015/>

16. Guardchild (n.d), 'Identity Theft Statistics', viewed 17 March 2016, < http://www.guardchild.com/identity-theft-statistics/>

17. Harrell, E. (2015). Victimcs of Identity Theft, 2014. US Department of Justice. USA. Avaiable URL: https://www.bjs.gov/content/pub/pdf/vit14.pdf

18. Hoar, S (2001), 'Identity Theft: The Crime of the New Millennium', HeinOnline, viewed 17 March 2016, < http://heinonline.org/HOL/LandingPage?handle=hein.journals/orglr80&div=34&id=&page=>

19. IT-Analysis, (2003). The Register. [Online]
Available at: http://www.theregister.co.uk/2003/12/04the_growing_problem_of_identity/
[Accessed 18 March 2016].

20. Jones, R (2014), 'Cybercrime now becoming a serious problem for many Britons', The Guardian, viewed 17 March 2016, < http://www.theguardian.com/money/2014/oct/21/cybercrime-identity-theft-hacking-abuse-social-media-britons>

21. Leon, J (2015), 'Identity Theft victim warns UAE public', Gulf News, viewed on 21 March 2016, <http://gulfnews.com/news/uae/crime/identity-theft-victim-warns-uae-public-1.1591776>

22. Lewis, K 2016, 'How Social Media Networks Facilitate Identity Theft and Fraud', Entrepreneurs' Organization, accessed on 15 February 2016, <https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud>

23. Liu, A 2014, 'The history of social networking', Digital Trends, accessed 15 February 2016, < http://www.digitaltrends.com/features/the-history-of-social-networking/>

24. Maceda, C (2011), 'Identity theft: Check credit card fraud and misuse', Gulf News, viewed on 21 march 2016, <http://gulfnews.com/business/identity-theft-check-credit-card-fraud-and-misuse-1.767763>

25. Marron, D (2007), 'Alter Reality', The British Journal of Criminology', Vol. 48, Issue No. 1, pp. 20-38, viewed on 2 April 2016, < http://bjc.oxfordjournals.org.ezproxy.uow.edu.au/content/48/1/20.full#ref-75>

26. McGinley, S 2013, 'Hackers targeting social media, warns UAE police', ITP.net, accessed on 15 February 2016, <http://www.itp.net/594535-hackers-targeting-social-media-warns-uae-police>

27. Moise, A.C (2015), 'Identity Theft Committed through Internet', Juridical Current, 18, 2, pp. 118-125, Academic Search Complete, EBSCOhost, viewed 17 March 2016.

28. O'Connell, N, and Siassios A 2013, 'Legal risks for social media users in the UAE', accessed on 15 February 2016, < http://www.tamimi.com/en/magazine/law-update/section-5/october-3/legal-risks-for-social-media-users-in-the-uae.html>

29. OECD (2009), 'The Scope of Online Identity Theft', Online Identity Theft, OECD Publishing, viewed on 17 March 2016, http://dx.doi.org/10.1787/9789264056596-3-en

30. Ravensdale, E 2015, 'How Australian people and businesses are using social media', Sensis Social Media Report, accessed on 15 February 2016, <https://www.sensis.com.au/assets/PDFdirectory/Sensis_Social_Media_Report_2015.pdf>

31. Reznik, M., (2013). Toura Law Review. Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation, Volume 29, pp. 1-3.

32. Sharp T, Shreve-Neiger A, Fremouw W, Kane J, and Hutton S. (2004) 'Exploring the Psychological and Somatic Impact of Identity Theft'. Journal of Forensic Sciences 49. pp. 1-4.

33. Siciliano, R (2011), 'The 6 Types of Identity Theft' McAfee, viewed on 21 March 2016, <https://blogs.mcafee.com/consumer/family-safety/the-6-types-of-identity-theft/>

34. Sophia, M (2015), 'UAE users lost Dhs 5bn through cybercrime – report', Gulf Business, viewed on 17 March 2016, < http://www.gulfbusiness.com/articles/industry/technology/uae-users-lost-dhs-5bn-through-cybercrime-report/>

35. Statista 2015, 'Statistics and facts about Social Networks', accessed on 15 February 2016, <http://www.statista.com/topics/1164/social-networks/>

36. Stroup, J (2014), 'The 8 Types of Identity Theft', About Money, viewed on 21 March 2016, <http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm>

37. Stroup, J 2014, 'The 8 types of identity theft', About Money, accessed on 14 February 2016, <http://idtheft.about.com/od/Basics/a/The-8-Types-Of-Identity-Theft.htm>

38. The National 2013, 'Half of UAE teens are victims of cyber threats', accessed on 15 February 2016, <http://www.thenational.ae/uae/education/half-of-uae-teens-are-victims-of-cyber-threats>

39. UNICEF (2012), "Child Safety Online: Global challenges and strategies", viewed on 2nd April 2016, < http://www.unicef-irc.org/publications/pdf/

40. Zeadally, S and Tsikerdekis, M (2015), 'Detecting and Preventing Online Identity Deception in Social Networking Services', IEEE Internet Computing, 19, 3, pp. 41-49, Computers & Applied Sciences Complete, EBSCOhost, viewed 17 March 2016.