Committee: Special Conference on Social Media (SPECON)

Issue: Combating crime and fraud in social media platforms

Student Officer: George Kantzis

Position: President

INTRODUCTION

Since the introduction of the very first social media platforms in the late 1970s, social networks have rapidly evolved and have become a significant part in a lot of people's daily lives. For instance, in accordance with Facebook Statistics, there are currently 1,5 billion people worldwide who actively use Facebook, ranking it as the largest and most famous social media site, while as stated by Twitter Statistics another 320 million people use the network on an everyday basis.

However, with the rise of the popularity of social media, crimes and frauds committed by hackers and other "internet masters" have inevitably increased as well. As a result, it is not a coincidence that in 2012 the Guardian published that from 2008 until 2012 reports regarding crimes in social media have escalated up to 780%, since in compliance with police sources in 2008 there were only 556 reports, whereas in 2012 there were 4908. Consequently, it is of the utmost importance to diminish the rate of online crimes, thefts and frauds and to foster security in all social media platforms, because it is predicted that the more technology advances, the more people are to use the Internet and all its communication services.

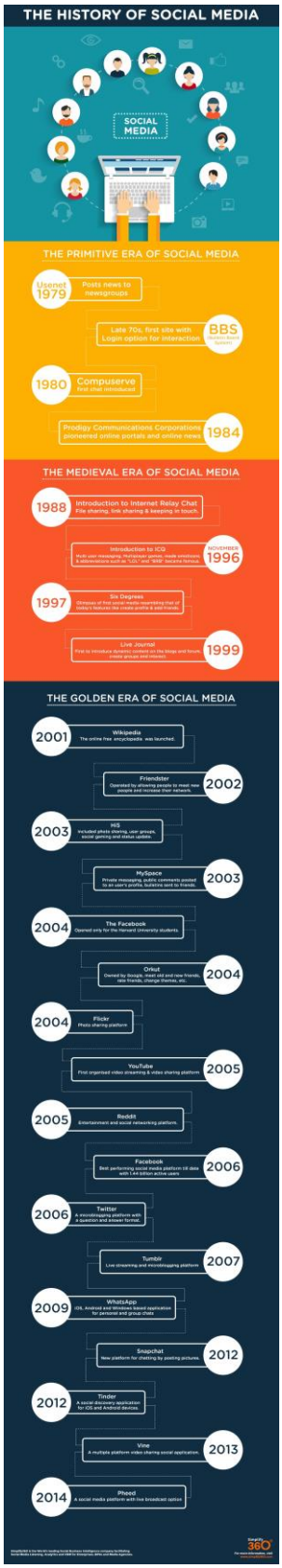

Figure 1: The history of social media from 1979 to 2014

DEFINITION OF KEY TERMS

Social Media

According to the "Business Dictionary" social media is defined as "internet or cellular phone-based applications and tools to share information among people. Social media includes popular networking

websites, like Facebook and Twitter; as well as bookmarking sites like Reddit. It involves blogging and forums and any aspect of an interactive presence that allows individuals the ability to engage in conversations with one another, often as a discussion over a particular blog post, news article, or event."[1]

Online Identity Theft

According to the "United States' Department of Justice", the term "online identity theft" is used "to refer to all types of crime, in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception on the internet, typically for economic gain."[2]

Internet Fraud

In accordance with the "Law Dictionary", "internet fraud" describes "a crime in which the perpetrator develops a scheme using one or more elements of the Internet to deprive a person of property or any interest, estate, or right by a false representation of a matter of fact, whether by providing misleading information or by the concealment of information."[3]

Cybercrime

Cybercrime is defined by the "Electronic Communications and Transactions Amendment Bill, 2012" as "any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them."[4]

Phishing

The Business Dictionary defines phishing as "the act of acquiring private or sensitive data from personal computers for use in fraudulent activities. Phishing is usually done by sending emails that seem to appear to come from credible sources, which require users to put in personal data such as a credit card number or social security number. This information is then transmitted to the hacker and utilized to commit acts of fraud."[5]

---

[1] "Social Media." *What Is Social Media?* BusinessDictionary.com, n.d. Web. 18 July 2016. <http://www.businessdictionary.com/definition/social-media.html>.
[2] "Identity Theft." *What Are Identity Theft and Identity Fraud?* U.S. Department of Justice, 2 Nov. 2015. Web. 18 July 2016. <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>.
[3] "Internet Fraud." *TheFreeDictionary.com*. N.p., n.d. Web. 18 July 2016. <http://legal-dictionary.thefreedictionary.com/Internet+Fraud>.
[4] "Cybercrime Definition." *Cybercrime.org.za*. N.p., n.d. Web. 18 July 2016. <http://cybercrime.org.za/definition>.
[5] "What Is Phishing?" *BusinessDictionary.com*. N.p., n.d. Web. 20 July 2016. <http://www.businessdictionary.com/definition/phishing.html>.

BACKGROUND INFORMATION

In the 21st century, the Internet and the online community have become a vital part of people's lives and hence each year there are even more users signed up in the social networks. Albeit social media platforms provide rapid, inexpensive and easy communication with a dispersed audience, they also present useful and sometimes also valuable information to criminal networks. In consequence, criminals utilize all resources found in social media, disguise themselves with anonymous online identities and contact their victims without much effort or many risks.

Identity Theft and Fraud in Social Media

As it has been mentioned earlier, the increasing number of social media users is highly correlated with the growing online attacks, frauds and crimes. However, how do social media networks facilitate the theft of identity and fraud? In order for one to answer that question, multiple factors have to be considered.

First of all, the main aspect that encourages and promotes fraudulent schemes is the absence of important information and knowledge that characterizes most social media users. Nowadays, there are many people of all ages that although not adequately informed about the dangers lurking online, continue to use social networks frequently and therefore put their personal identity at risk. Yet, this lack of knowledge is not entirely the consumers' fault, as there are generally limited incentives in the social community to offer education to users on such crucial issues, like cyber security and protection of privacy.

Secondly, the deficiency of online consciousness is associated with the thriving confidence and trust of consumers as regards the provision of personal data. It is known that social networks, such as but not limited to Facebook, suggest users provide as many personal details as possible. Through that way social media then analyze these pieces of information and as a result they solicit funds deriving from targeted advertisements about different products of interest to those users. However reasonable this strategy might seem, with the provision of confidential details, users are highly susceptible to fraud, as all their data are freely exposed in the cyberspace.

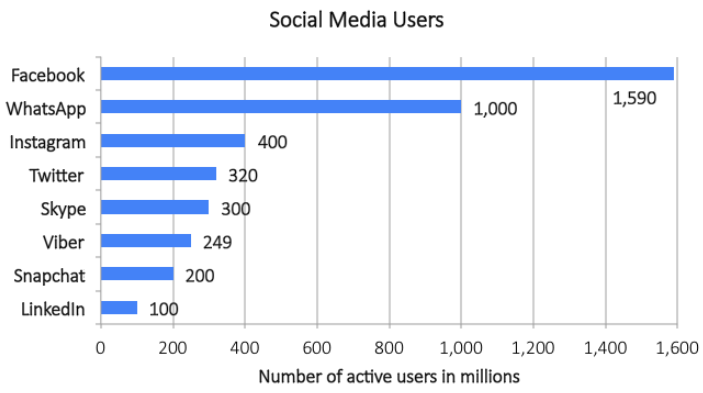

Figure 2: The number of active social media users in millions

Source of information: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Finally, it is evident that all social media platforms include innumerable private details, which are highly likely to be exposed via a hacker attack at the main server of the network. Hence, the request and use of personal information for the beneficial purposes of most social media companies facilitate identity theft and cyber fraud, as almost every user has his/her data publicly revealed with no precautions taken.

Crimes of Opportunity

A crime of opportunity is considered any crime that does not involve great risk or effort, but provides a good reward if the action is successful. For once again, the more people tend to use social media, the more and the better opportunities exist for fraudsters to commit online swindles and steal identities. Since the majority of online consumers update their status by posting pictures and other personal material, it is really uncomplicated for criminals to observe multiple accounts, to target specific people and to commit frauds without any obstacle. For instance, a lot of people utilize the "check-in" application in Facebook or Instagram, revealing their position on the world map. If they post that they are currently abroad, there is a high possibility that their residence might be burgled.

Figure 3: Social Media Services

Moreover, online platforms, such as Snapchat, YouTube and Flickr, which are based on the exchange or share of photos and videos, might imperil one's personal identity, since the perpetrator will have a deeper insight concerning someone's habits, favourite activities, friends and relatives. Lastly, data such as hometown, school, full name and date of birth, can also be used against the consumers in various malicious ways. It is therefore obvious, that social media platforms encourage crimes of opportunity, because offenders can acquire all the necessary information to commence their abuse without having to overcome strenuous barriers and perilous risks.

Cybercrimes

The term cybercrime is used to describe a range of different criminal activities through the Internet. According to "Norton by Symantec", a worldwide renowned anti-virus company, cybercrime can manifest itself in different methods, such as "the theft of personal

data; the infringement of copyright; fraud; identity theft; child pornography; cyber stalking; cyber bullying and hacking"[6]. By and large, cybercrime is divided into two subcategories based on the skills needed and the methods followed.

On the one hand, cybercrime type one revolves around the spread and the installation of viruses in other computers or laptops. For example, the victim can accidentally download a virus without noticing, and thus allow the hacker to steal sensitive data. Furthermore, type one may also refer to the method of "phishing", in other words hackers claiming to represent a legal company send and email with an attached link that may lead to a website which can damage the computer client. Last but not least, cybercrime type one generally relates to the manipulation of websites, services and personal data through methods such as identity theft, hacking, viruses and fraud.

On the other hand, cybercrime type two is more severe, owing to the fact that it encompasses crimes, like cyber stalking, child pornography, blackmailing, espionage and terrorist attacks. A common example of cybercrime type two would be the constant blackmailing of a person via chat rooms to do a specific action that may lead to his/her humiliation, exploitation, harassment or exposure.

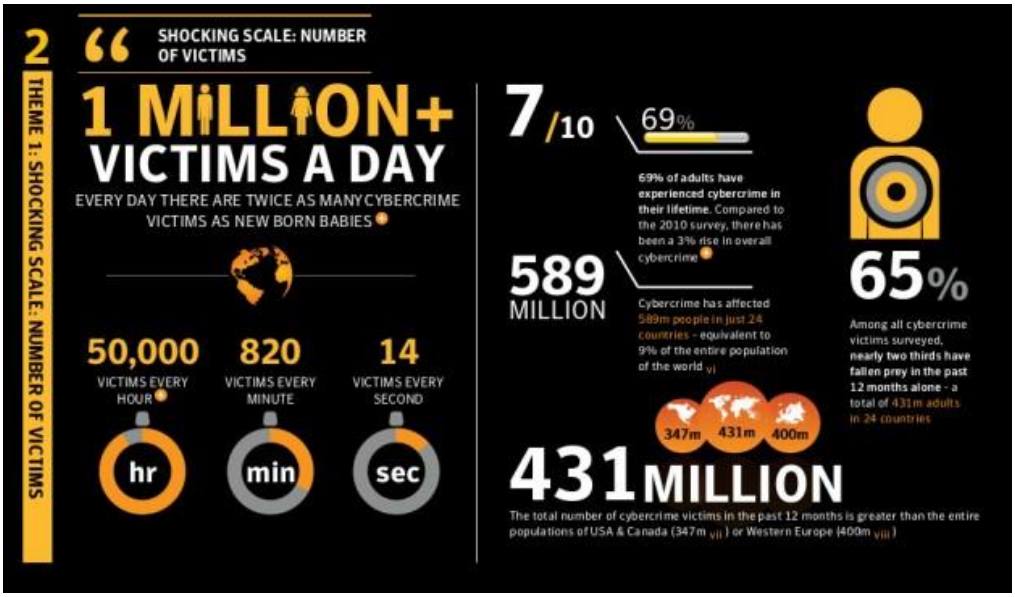

Figure 4: Every day there are twice as many cybercrime victims as newborn babies. The total number of cybercrime victims in the past 12 months is greater than the entire population of the USA and Canada, namely 431 million victims

To sum up, cybercrime in all its forms, online crimes of opportunity and identity theft are all common offences which have critical reverberations as regards the safety of online users around the world. As a consequence, it is imperative that governments apply strict regulations to combat these malfeasances, enhance cyber security and protect their citizens.

[6] "What Is Cybercrime?" *Cybercrime*. Norton by Symantec, n.d. Web. 18 July 2016. <http://us.norton.com/cybercrime-definition>.

MAJOR COUNTRIES AND ORGANISATIONS INVOLVED

Commonwealth of Canada

Canada has signed the Council of Europe's "Convention on Cybercrime" and therefore denounces cybercrime and other frauds in social media platforms. Nevertheless, social media are used by Canadian police forces to send crime alerts, to provide information regarding lost persons and to upload photos of crime perpetrators to facilitate their identification. Lastly, in 2000 the Canadian Government distributed a document to all Justice Ministers condemning cybercrimes and especially child pornography and online identity theft.

People's Republic of China

China is also suffering from extensive cybercrime and online fraud for over three decades. In 1994, China published its first national legislation regarding online crimes. In 2001, the Government issued the "New China Criminal Legislations in the Progress of Harmonization of Criminal Legislation Against Cybercrime", so as to combat cybercrime and frauds in the cyberspace. In accordance with Reuters, in August 2015 Chinese Police Forces incarcerated 15.000 people for online crimes who have endangered China's Cyber Security System.

French Republic (France)

The computer security company Symantec claims "the French suffer more from cybercrime than any other Europeans, since it has reported that 41% of French smartphone users have been victims of criminal acts in the past year compared to 29% in Europe and 38% worldwide."[7] Although France has signed the "Convention on Cybercrime" of the Council of Europe, the country still continues to be a target of mass cyber attacks and social media frauds.

Federal Republic of Germany

Germany has also signed the "Convention on Cybercrime" and actively condemns online fraud in social media networks and other cybercrimes. In addition to that, because of the need of further laws to eradicate crimes and frauds in social media, Germany implemented a new set of regulations in 2007 which officially criminalized all forms of cybercrime, thus significantly decreasing online fraud and identity theft in its territory.

---

[7] Rfi. "France Has Most Cybercrime Victims in Europe." *RFI*. The World and All Its Voices, 03 Oct. 2013. Web. 19 July 2016. <http://en.rfi.fr/economy/20131003-france-has-highest-cybercrime-rate-europe>.

Russian Federation

Russia has not ratified the "Convention on Cybercrime" of the Council of Europe yet and therefore cybercrime rates are really high. For this reason, Russia should implement stricter measures that are compatible with the international law and effectively tackle the issue of online crime and fraud.

United Kingdom

The United Kingdom is also a signatory of the "Convention on Cybercrime". In the last years, the UK mainly focuses on the protection of children from online crimes, such as child pornography and harassment and cyber bullying via social media platforms and hence has maintained a normal level of cyber security.

United States of America

According to the FBI, "the key priorities of the US government are combating computer network intrusions, identity theft and fraud."[8] It is apparent that cybercrime poses a huge danger to the United States, as the government often combines cybercrime with terrorism. Through this combination and the joint fight of both offences, the country has observed advantageous results. Finally, the USA has also ratified the "Convention on Cybercrime".

International Telecommunication Union (ITU)

The International Telecommunication Union has been an active organization fighting crimes and frauds in social media. In 2012, ITU published a report with the title "Understanding cybercrime: Phenomena, challenges and legal responses". The document covered all possible aspects of cybercrime and included strategies that have to be adopted and frameworks that should be implemented.

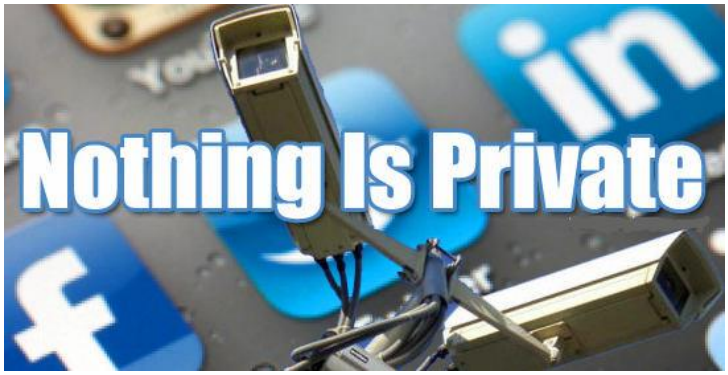

Figure 5: All people using social media platforms are equally susceptible to cybercrime and online frauds

[8] "Cyber Crime." *FBI*. FBI, n.d. Web. 19 July 2016. <https://www.fbi.gov/investigate/cyber>.

TIMELINE OF EVENTS

Date	Description of Event
1979	The Primitive Era of Social Media starts with the introduction of the Usenet, which posts news to existing newsgroups.
1988	File and link sharing and communication via the “Internet Relay Chat” are made available.
1990s	Search engines, like Google, were introduced and theft identity became a common issue.
2001	The Council of Europe adopts the first international “Convention on Cybercrime”
2012	The Guardian published a report indicating that online crimes have risen up to 780% compared to the cybercrimes in 2008.
February 2013	“The United Nations Office on Drugs and Crime” (UNODC) released its report on cybercrime.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

- United Nations General Assembly Resolution 65/230, which mandated the creation of the UN Cybercrime Study.
- United Nations General Assembly Resolution 55/63 of 2001, called “Combatting the criminal misuse of information technologies”.
- The “Comprehensive Study on Cybercrime” adopted in February 2013 by UNODC aims to emphasize the importance of the situation and to recommend global legislative programs to tackle the issue.
- The Economic and Social Council Resolution 2011/33, which deals with the topic of the misuse of the internet and other information technologies to abuse, fraud and exploit children.
- The “Convention on Cybercrime” was introduced in Budapest on the 23rd of November 2001 by the Council of Europe. This Convention is thought to be the first legally binding international treaty on the issue of cybercrime and online fraud. As it is stated in the pre-ambulatory clauses, the aim of the Convention is to create a legal background with specific and applicable laws and measures combatting cybercrime and to endorse international cooperation on this matter. Nowadays, the Convention has been signed by a total number of 50 nations throughout the world.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

In the past years, the immense growth of Internet's popularity in conjunction with the increase of cybercrimes and fraud in social media networks have led to the necessity for strong legislations. Numerous measures have been adopted and many attempts to counter the problem have been made, both by international organizations and by regional institutions.

Figure 6: The most famous social media networks are the top targets for online fraud

First of all, the United Nations has made great progress in addressing the problem of cybercrime in its resolutions in the General Assembly and the Economic and Social Council (ECOSOC). Since 2000, a number of resolutions have passed covering multifarious features of the problem. For instance, in 2001 the UNGA adopted the resolution A/RES/55/63, which emphasized the importance that countries should coordinately investigate and condemn social media crimes. In addition, GA resolutions, such as A/RES/56/121 and A/RES/63/195, stress out that combatting cybercrime will have a positive impact on other international organized crimes, like terrorist operations and attacks.

Secondly, the European Union (EU) has also created a legal document concerning cybercrime called the "Convention on Cybercrime", which was officially enforced in 2004. The Convention included measures to combat child pornography, fraud, forgery and identity theft, copyright violations and illegal access to personal data in social media platforms. Additionally, many other regional organizations, namely the "Organization of American States (OAS)", the "Asia-Pacific Economic Cooperation (APEC)" and the "Economic Community of West African States (ECOWAS)", have also played a significant role in eliminating online frauds and crimes.

However, cyber security has not yet been fully established and as such frauds and crimes continue to happen in the cyberspace. Last but not least, it has been observed that countries have been roughly divided into two main strongholds, the Less Economically Developed Countries (LEDCs) and the More Economically Developed Countries (MEDCs). The former argue that measures shall predominantly deal with child pornography and other violations, whereas the latter most times claim that measures shall first prohibit piracy and frauds, since both can affect the businesses and the production chain. Although these

differences still exist to some extent, countries have to stand united and implement laws that eliminate all cybercrimes and frauds in social media.

POSSIBLE SOLUTIONS

Crime and fraud in social media platforms are universal phenomena, which have serious implications regarding the maintenance of cyber security. Consequently, countries shall propose explicit laws focusing on each and every facet of the issue, namely not only prohibiting cybercrimes, such as child pornography and cyber bullying, but also preventing online frauds, scams and identity theft scandals. To achieve this, there are two different approaches that could be followed.

Firstly, social media companies, like Facebook, Twitter, Instagram and YouTube, can combat online fraud and crime by adopting extra security measures. For example, social networks have to update their security protocols regularly and run frequent online investigations so as to track and avert suspicious online actions. Moreover, social media companies can also encourage their users to change their access passwords habitually and can provide online account security examinations to hinder the installation of viruses and the revelation of their personal information.

Figure 7: Online fraud is detrimental to the maintenance cyber security

Secondly, the problem must be addressed on a national and governmental level as well. Each government has to promote education for the young generations on the correct and safe use of social media in order for people to be able to prevent cybercrimes and public exposure. In particular, public institutions cooperating with the government could organize lectures, seminars and other interactive courses, where people could learn how to protect their sensitive personal data, what dangers may lurk in the cyberspace and how to avoid frauds, hacking and other types of cybercrime in their social media accounts.

To conclude, eliminating social media frauds and crimes are of the utmost importance, since the eradication of such offences will result in the prevalence and the improvement of cyber security.

BIBLIOGRAPHY

"4 Case Studies in Fraud: Social Media and Identity Theft." *Socialnomics*. N.p., 13 Jan. 2016. Web. 18 July 2016. <http://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/>.

"Chinese Police Arrest 15,000 for Internet Crimes." *Reuters*. Thomson Reuters, 18 Aug. 2015. Web. 20 July 2016. <http://www.reuters.com/article/us-china-internet-idUSKCN0QN1A520150818>.

"Comprehensive Study on Cybercrime." *UNODC.org*. N.p., Feb. 2013. Web. 19 July 2016. <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>.

"Convention on Cybercrime." *Council of Europe*. N.p., 23 Nov. 2001. Web. 19 July 2016. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561>.

"Convention on Cybercrime." *Council of Europe*. Treaty Office, n.d. Web. 19 July 2016. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185?_coeconventions_WAR_coeconventionsportlet_languageId=en_GB>.

"Cyber Crime." *Cross Domain Solutions*. WordPress, n.d. Web. 20 July 2016. <http://www.crossdomainsolutions.com/cyber-crime/>.

"Cyber Crime." *FBI*. FBI, n.d. Web. 19 July 2016. <https://www.fbi.gov/investigate/cyber>.

"Cybercrime Definition." *Cybercrime.org.za*. N.p., n.d. Web. 18 July 2016. <http://cybercrime.org.za/definition>.

"France Has Most Cybercrime Victims in Europe." *RFI*. The World and All Its Voices, 03 Oct. 2013. Web. 19 July 2016. <http://en.rfi.fr/economy/20131003-france-has-highest-cybercrime-rate-europe>.

"Identity Theft." *What Are Identity Theft and Identity Fraud?* U.S. Department of Justice, 2 Nov. 2015. Web. 18 July 2016. <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>.

"Internet and Social Media Fraud." *Investor.gov*. USA Securities and Exchange Commission, n.d. Web. 20 July 2016. <https://www.investor.gov/investing-basics/avoiding-fraud/types-fraud/internet-social-media-fraud>.

"Internet Fraud." *TheFreeDictionary.com*. N.p., n.d. Web. 18 July 2016. <http://legal-dictionary.thefreedictionary.com/Internet+Fraud>.

"Prevention, Protection and International Cooperation against the Use of New Information Technologies to Abuse And/or Exploit Children." *UNODC.org*. UNODC, n.d. Web. 19 July 2016. <https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2011/ECOSOC/Resolution_2011-33.pdf>.

"Social Media-related Crime Reports up 780% in Four Years." *The Guardian*. Guardian News and Media, 27 Dec. 2012. Web. 18 July 2016. <https://www.theguardian.com/media/2012/dec/27/social-media-crime-facebook-twitter>.

"Social Media." *What Is Social Media?* BusinessDictionary.com, n.d. Web. 18 July 2016. <http://www.businessdictionary.com/definition/social-media.html>.

"Twelfth United Nations Congress on Crime Prevention and Criminal Justice." *UNODC.org*. General Assembly Resolution 65/230, n.d. Web. 19 July 2016. <https://www.unodc.org/documents/justice-and-prison-reform/AGMs/General_Assembly_resolution_65-230_E.pdf>.

"What Is Cybercrime?" *Cybercrime*. Norton by Symantec, n.d. Web. 18 July 2016. <http://us.norton.com/cybercrime-definition>.

"What Is Phishing?" *BusinessDictionary.com*. N.p., n.d. Web. 20 July 2016. <http://www.businessdictionary.com/definition/phishing.html>.

Harden, Seth. "Facebook Statistics." *Statistic Brain*. N.p., 19 June 2016. Web. 19 July 2016. <http://www.statisticbrain.com/facebook-statistics/>.

Hoscheidt, Matheus M., and Elisa Felber Eichner. "Legal and Political Measures to Address Cybercrime." UFRGSMUN, 2014. Web. 20 July 2016. <https://www.ufrgs.br/ufrgsmun/2014/files/WSI2.pdf>.

Kent, Lewis. "How Social Media Networks Facilitate Identity Theft and Fraud." *How Social Media Networks Facilitate Identity Theft and Fraud*. N.p., n.d. Web. 20 July 2016. <https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud>.

Sheena. "How Cops Use Social Media to Fight Crime and Cyberbullying." *Careermash.ca*. N.p., 13 Feb. 2012. Web. 20 July 2016. <http://careermash.ca/blogs/how-cops-use-social-media-fight-crime-and-cyberbullying>.

FIGURES' BIBLIOGRAPHY

Figure 1: http://www.adweek.com/socialtimes/wp-content/uploads/sites/2/2015/05/SM-Infographics.jpg

Figure 2: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Figure 3: https://conversationprism.com/wp-content/uploads/2014/11/JESS3_BrianSolis_ConversationPrism4_WEB_1600x1200.jpg

Figure 4: http://icdn4.digitaltrends.com/image/950-cybercrime-scale-964x563.jpg

Figure 5: http://aworkcovervictimsdiary.com/wp-content/uploads/2013/07/soacila-media-surveillance-workcover.jpg

Figure 6: http://www.iiiweb.net/wp-content/uploads/2014/06/Social-Media-Posts-Lead-to-Proof-of-Insurance-Fraud.jpg

Figure 7: http://www.visiblebanking.com/wp-content/uploads/2012/09/fraud-risk-mgmt.jpg