PHISHING AND PHARMING AS FORMS OF IDENTITY THEFT AND IDENTITY ABUSE

Vida M. VILIĆ
PhD, Clinic of Dentistry Niš, Assistant Director for Legal Matters,
vila979@gmail.com

Abstract
Identity theft in cyberspace can have significant consequences, considering the fact that most of the victims of cyber identity theft do not immediately recognize that something has been stolen from them. There are various ways cyber identity theft is carried out, the most common being phishing and pharming.
A small number of countries have passed criminal legislation that specifically regulates and sanction identity theft as a criminal offense, though most countries do treat identity theft as a form of illegal access to data, fraud, forgery, or copyright infringement, or as an act that precedes the commission of another criminal offense. Serbia falls into the second category. The current criminal legislation of Serbia does not specifically criminalize the act of identity theft using the Internet and social networks. If any form of identity theft occurs, the provisions of the Criminal Code relating to computer fraud, fraud, forgery and misuse of payment cards, unauthorized use of another's name and other special markings of goods or services shall apply.
In addition to defining the terms of identity theft and identity abuse and analysis of phishing and pharming as the most common phenomena of cyber identity theft, this paper also presents the current applicable legislation in Serbia, with critical review, as well as international measures of protection against such criminal behavior in cyber space.

Key words: *identity, identity theft in cyberspace, identity abuse, criminal offense*

Introduction

A person's identity is a set of characteristics related to that specific individual, which "characterize the individual and by which that individual differs from other persons" (Milićević & Vujović, 2012, p. 303). In addition to legal changeable properties such as personal name, surname, citizenship, or marital status, factual unchangeable properties such as date and place of birth, registry number, or social security number, and physical properties such as gender, physical appearance there are also virtual properties that every an individual have, such as passwords, different virtual user names, credit card

pin codes. All identifying information can be misused and if it is the right to privacy of internet and social network users is violated.

Identity theft through the use of the internet can have significant consequences, such as financial losses or use or abuse of private and confidential user information in order for someone to obtain false documents. These consequents are all the more problematic because most victims of identity theft are not immediately able to recognize that something has been stolen from them. Although there are no precise data on the frequency of the criminal offense of identity theft, some US research has found that in the past five years, one in eight US citizens has been the victim of internet identity theft (Beal, 2012).

Identity theft and identity abuse

According to the definition of identity theft given by Gross & Acquisti, the identity theft consists of "the unauthorized use of personal data (date of birth, current residence, phone number, occupation, friends, personal images) that has become publicly available" (Gross & Acquisti, 2005, p.80). Roberts considers that identity theft "involves the online misappropriation of identity tokens (e.g. email addresses, webpages and the combination of username and password used to access systems), typically for financial gain" (Roberts, 2008, p. 2). Defining the term itself, identity theft in cyberspace is described as "a form of fraud by using personal and financial data from a computer, obtained through a false e-mail or website. When preforming the act of identity theft, a person falsely presents himself as another person with the intention of obtaining illegal and unauthorized material gain or other personal gain" (Bidwell, 2002, p.3, Ivanović, Uljanov & Urošević, 2012, p.149).

Identity theft begins with the acquisition of personal information of a person, without the knowledge and consent of that person, through acts of deception, theft or fraud, and continues with the use of collected data for the commission of any other criminal acts, that in most often related to illegal material gain for the perpetrators (Milošević & Urošević, 2009, p. 55). Certain authors perceive identity theft as taking over someone's "role" on the internet in order to gain some material or other benefits (Prlja & Reljanović, 2009, p. 169). This is one of the most drastic attack on personality and someone's privacy, which presupposes the prior execution of another criminal offense such as fraud, intrusion into a computer or computer system, virus or other malware. Identity theft can also be defined as "unauthorized collection, transfer, retention or use of information relating to a natural or a juridical person for the purposes of perpetrating further crimes such as theft, fraud and other similar crimes through computer systems and networks" (Cradduck, 2007 cited in Abdul Manap, Abdul Rahim & Taji, 2015, p.599), which "makes it a two-stage crime: unauthorized collection of personal information

and the fraudulent use of this information in order to secure a benefit to the detriment of the owners" (Abdul Manap, Abdul Rahim & Taji, 2015, p.600).

Some of the most influential international organizations, also tried to define and to regulate this criminal act through their strategy documents. The 12th UN Congress on Crime Prevention and Criminal Justice, held in 2010, defined identity theft as "the misuse of personal data of another person with the intention of fraud" (12th UN Congress on Crime Prevention and Criminal Justice, 2010:12). The OECD indicates that identity theft occurs "when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes" ("OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft", 2007, p. 3). In order to take someone's identity and obtain personal information about an individual, perpetrators use different methods: sending and activating malicious programs, sending e-mails of misleading content, or referring a person to false internet sites that mislead the visitor to record their personal data. When one's personal data is taken in such an unauthorised manner, it can be misused in various ways; the most common is the abuse of bank accounts, the opening false accounts, the illegal use of the data gathered by certain state authorities, services and documents, fraud related to health insurance ("OECD Ministerial meeting on the future of the internet economy", 2007, p. 4).

In 2007, the Council of Europe prepared a platform for the development of a unified, universal legislation on identity theft, defined as "misappropriation of the identity of another person, without their knowledge or consent", such as identifying features of a person or a significant part thereof, no matter the owner is alive, real or fictional person, or has died ("Cybercrime Convention Committee – T-CY Guidance Note #4, Identity theft and phishing in relation to fraud, Council of Europe", 2013). Identity theft usually consists of three elements: the mode of execution of the act itself (modus operandi), the target of attack and the motivation of the perpetrator. The most common modus operandi are physical method including computer theft, illegal seizure of data carriers, electronic mail theft, use of internet browsers and file sharing systems, hacker attacks, and attacks by social engineering. The most common targets of identity theft attacks are identification numbers (e.g. Unique citizen registration number, social security number), personal identification numbers (ID number, passport number, credit or debit card number), user names and passwords on different internet accounts. There are a number of different motivations for the criminal act. It is usually aimed at acquiring material gain, concealing the someone's true identity or as a preparatory action for the commission of another criminal offense.

Phishing and pharming, as forms of identity theft and identity abuse

Identity theft perpetrators most often achieve their goal by using social networks to collect passwords, user names and credit card numbers from a computer that the victim often use. Each computer collects information that the user enters and stores, and this information stays hidden on the hard disk during the use of various programs and services. Files that are hidden on the computer, such as in cache, history and other temporary internet files, can be used in order to reconstruct the user's internet habits. It is these files that store information like user names and passwords, names, addresses, credit card numbers.

There are various identity theft *modus operandi*, such as hacking, phishing, pharming, spoofing, which is unauthorized access to an internet site in order to reach other persons'important data, skimming, which is fraud by using debit or credit cards in the sense of storing information gathered from the magnetic stripe of the card itself and then use them for making a forgered card, scamming, which are types of scams and frauds sent through e-mails, most often in the form of false lotteries, phishing messages, so called "Nigerian scam", redirecting the data to the wrong electronic address, filling false forms on the internet, false log entries using confidential passwords in order to enter on the different profiles (Paget, 2007). However, the most common form of theft of someone's identity and confidential information via email is the called phishing.

Identity theft using e-mail, phishing, consists in sending an e-mail to the user, indicating that the message is sent by a legitimate legal entity or an authorized person, seeking personal, confidential and private information. The allegations in the message are fake, and if the recipient writes the information they are looking for, it will later be used for identity theft. This way, the user provides the perpetrator with secure personal information, like user name, password, credit card number, so the perpetrator can download the identity of the user in some form of electronic communication. This kind of email directs users to visit a website where they are asked to update their personal information, like passwords and credit card numbers, social security number, bank account numbers. The website is, however, fake and configured only for theft of user information ("All about phishing", 2006).

There are various ways in which such abuse can be carried out,[1] and the social engineering scheme[2] consists of three stages of execution the criminal

[1] An electronic message typically contains some of the following elements: the "from" field appears to be referred to as a legitimate company mention usually in the subject of an email. An email typically contains a logo and images taken from a mentioned company's web site. An email usually contains a link through which it is necessary to enter the personal information of the e-mail owner.

act: in the first phase, the perpetrator sends an email to the potential victim, and the message appears to be sent on behalf of the bank that victim uses or on behalf of another an organization that could be close to the victim and which may require certain personal data; the second phase begins when the victim reads an email, responds to it, or forward the message to the corresponding false internet site, leaving certain personal data and *the* third phase involves forwarding of the victim's data directly to the perpetrator, who uses the obtained data to perform some other illegal or criminal act, which most commonly are considered as the offense of fraud ("OECD Ministerial meeting on the future of the internet economy", 2007, p. 17).

Phishing techniques can include identity theft using malicious software (so-called *pharming*) and *targeted* phishing ("OECD Ministerial meeting on the future of the internet economy", 2007, p. 16):

(1) Identity theft using malicious software (*pharming*) is a special form of phishing in which a hacker attempts to redirect electronic communication and data from a legitimate website to a completely different internet address. This type of abuse is usually performed by changing files on a user's computer or by exploiting the shortcomings on the server that the victim has been used. This is a more sophisticated type of phishing, because in this case, the user should not reply to the email that would provide the perpetrator with all private and confidential data of the user. Only by opening such an electronic message, the computer virus, Troyan, malware or a key generator is downloaded to the victims' computer, stealing all victims' important data - passwords, user names and credit card numbers used on that computer (Beal, 2016). After obtaining data, it is possible to create false identifications, forge documents, checks or credit cards.

(2) Opposite to the "regular" phishing, *targeted phishing* (or so called "spear phishing") is not about sending electronic messages to the masses, but

Usually, the email will indicate the result of the non-activation of the link from the message, for example "Your account will be suspended or closed". Such an email may contain a logo that is not the same as the company logo, spell-checking errors, the "%" sign of the tracked number, or "@" characters in the hyperlinks, random names or email addresses in the body of the text or the header of the email. See: All about phishing.

[2]Social engineering represents the method of bringing the victim into the situation to reveal certain confidential information to persons who are not authorized to know them, that is originally phishing attack by using misleading or fake emails and "hacked" websites of companies and banks, designed to "make" the user to give certain personal, private and identification information. (See more in Prlja, Ivanović & Reljanović, *Krivična dela visokotehnološkog kriminala*. Institut za uporedno pravo, Beograd, 2011, p.116)

to the victims well selected according to some preferences or habits, and therefore this kind of targeting is much more precise. This type of "phishing" is directed to specific groups of Internet users or even to specific individuals. These kind of phishing attempts are not typically initiated by random hackers, but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information ("Spear phishing", 2019). Instead of sending the phishing emails to a large group of people, the attacker targets a select group or an individual, making the malicious emails seem more trustworthy.

Phishing and pharming can have significant consequences.[3] Most common are the documents with one person's (victim) data and the photo of the perpetrator (Beal, 2016). The social network users must protect themselves by carefully choosing their friends and contacts in the cyber space. Security firm "Sophos" (n.d.) conducted an interesting research in order to demonstrate the "ugly side" of the use of the social networks, the possibilities of their abuse and the unreasonableness of the users themselves. Two false profiles were created on Facebook: the first profile was registered on the user named Daisy Feletin, 25 years old woman, who had a rubber duck figure in the profile picture, and the second profile was registered on the user named Dinette Stonily, about 50 years old, who had as the profile picture the image of a playing kitten. The research focussed on Facebook users from Australia, and each of these two false Facebook profiles sent 100 friend requests to different people. In general, 87 out of 100 contacted Facebook users responded positively to send friend requests, and the curiosity is that another 5 people who were not directly contacted sent a friend request to these two fictitious user profiles. It is interesting how much personal data has been exchanged during the communication between these "cyber friends": over 87% made their e-mail address available, and 23% of the younger and 7% of the older internet users gave their phone number to a fictitious "friend". Forty-six percent of younger users and 31% of the elderly shared personal information about themselves and their family members, while 89% of the younger and 57% of the elderly wrote their full date of birth during the communication.

The OECD pointed to some of the major issues faced by all countries when resolving the problem of identity theft: the lack of a unique definition of this offence, non-existance of the legal provisions related to identity theft as a criminal offense *per se* in national legislation, improvement of the

[3]Although there are no precise data on the frequency of the criminal offence of identity theft, some US research has found that in the past five years, one in eight US citizens has been the victim of Internet identity theft. *See:* Internet Identity Theft (n.d.).

cooperation with the private sector, the lack of indicative statistics on the extent and the structure of this criminal act, the lack of victim assistance programs and appropriate legal remedies, inadequate education of social network users, which may lead to identity theft ("OECD Ministerial meeting on the future of the internet economy", 2007, p. 5).

Certain authors, like Newman & McNally (2005, p. vi) consider that recording and reporting of identity theft as a crime has been determined by three significant issues: (1) problem in defining identity theft because of its extensive involvement in other crimes; (2) transnational nature of identity theft that led to jurisdictional confusion as to whose responsibility it is to record the crime and (3) individuals, who are more likely to report their victimization to state agencies and public services instead to the police.

The legislation of identity theft worldwide and in Republic of Serbia

A small number of countries have passed criminal legislation that specifically regulates and sanctions identity theft as a criminal offense, while most of the countries treat identity theft as a form of illegal access to data, fraud, forgery, copyright infringement etc. or as an act that precedes the commission of another criminal offense.

Concerning the fact that identity theft has numerous elements and variations, most of the countries relate identity theft as privacy violations and sanction it as part of the unauthorized collection and use of personal data, illegal access to data, fraud, forgery, copyright infringement, or as acts that precede to the commission of another criminal offense. The European countries of Austria, Bulgaria, Belgium, Hungary, Greece, Germany, Ireland, Italy, The Netherlands, Poland, Romania, Spain do not have identity theft as a specific crime in their legislation (Robinson, Graux, Parrilli, Klautzer & Valeri, 2011, p. ix), but have prescribed the provisions in other legal documents that may apply to the cases of identity theft.

As a criminal offense *per se*, the identity theft is regulated by the United States Identity Theft and Assumption Deterrence Act (1998). Canada and the United Kingdom also legally regulate and sanction identity theft as a criminal offense, with the legal practice to pursue and sanction these criminal acts as fraud or forgery (Canadian Department of Justice, 2007).

In the United Kingdom, identity theft is treated as a form of fraud that can be committed on the Internet in one of the following ways: false representation, failing to disclose information or abuse of position (The UK Fraud Act, 2006; "Out-Law news: Phishing kits banned by new Fraud Act", 2015). In 2005, France attempted to introduce identity theft as a criminal offense in its criminal justice system, but in 2006 this proposal was withdrawn from the procedure, with the expanation that this behavior was already a crime by virtue of the fact that is was undertaken in the process of committing

other crimes ("OECD Ministerial meeting on the future of the internet economy", 2007, p.16). However, in 2011, the Criminal Code of France criminalized identity theft as a particular criminal offense (Article 434-23), which exists if two conditions are met: first, the perpetrator has to (mis)use the name or email address of another living person, and second, the potential victim of identity theft can be legally prosecuted because the real perpetrator used the identity of the victim to commit certain criminal act. The criminal offense of identity theft, according to the legal text, consists of two elements: the use of some else's identity or personal data which allows the identification of that person in electronic communications (material element) and the intent to disturb the peace of the victim or to impinge the reputation or honor of the victim (the element of intent) (Robinson, et. al., 2011, p. 268).

Some international organizations took an active part in combating cybercrime through their practical work, legal initiatives and their adopted and ratified legal documents. Some of them are also connected to identity theft and the affirmative action of police forces and judicial authorities. Interpol was the first international organization to exert considerable effort against this crime. The Third Interpol Symposium on International Fraud, held in Paris in 1979, was convened to find mechanisms for the legal regulation and prevention of computer crime. This organization warned about the huge threats of computer-related crime and provided operational manuals which contained the latest information and instructions for prosecutors and police teams. The UN fight against cybercrime is carried out within several UN organizations, primarily through the United Nations Office on Drugs and Crime (UNODC, 1997)[4] and the United Nations Office for Disarmament Affairs (UNODA, 2016). The UNODC particularly deals with the criminal misuse of identity and identity theft, promotion of high-tech offenses legislation, and the police and prosecuting authorities' staff training. The UNODA, among other activities, deals with issues related to information warfare and cyber terrorism.

The current criminal legislation of Serbia does not specifically criminalize act of identity theft using the Internet and social networks. Identity theft, as related to privacy, is regulated indirectly, through legal provisions relating to the protection of privacy. This form of illegal behavior is not comprehensively considered nor are the most common forms of its manifestation described. In criminal legislation, identity theft is not formulated as a separate criminal offense, but is cited as one of the forms of

[4]The Organization was founded in 1997, with the aim of solving international problems concerning illegal drug trade, preventing criminality and fighting against international terrorism (See: *United Nations Office of Drugs and Crime*)

personal data misuse. If identity theft occurs, the provisions of the Criminal Code of the Republic of Serbia (Krivični zakonik Republike Srbije, 2005) relating to computer fraud (Article 301), fraud (Article 208), forgery and misuse of payment cards (Article 255, paragraph 4), unauthorized use of another's business name and other special marking of goods or services (Article 233) are applicable. The Code also protects the right to privacy; any violation of the right to privacy by the authorities, other individuals and institutions, including the persons working in mass communications, is a crime. All criminal offenses have different object of attack (personal appearence or a photography, personal address, the reputation of an individual, personal letter, parcels, file, electronic records or data, personal computer), but the same general object of protection - privacy.

Personal Data Protection Act (Zakon o zaštiti podataka o ličnosti, 2008), among other things, regulates the conditions for the collection and processing of personal data and the rights of the individual to protect his/her personal data. The Personal Data Protection Act declares that the existing legal regulations are not sufficient when it comes to defining the mechanisms for protecting the Internet users in general, particularly regarding the users of social networking sites, who willingly leave their personal data, thus making them available to the millions of Internet users throughout the world (Vilić & Radenković, 2016: 62). However, this Act does not apply to data that are available to everyone and published in publications and on social networks, as well as to data that somebody has willingly published about himself and therefore does not correct the insufficiency of previous laws (Vilić & Radenković, 2015: 340).

The largest databases of personal information are maintained by the Ministry of Internal Affairs in the form of records on personal identification cards, the Republic Health Insurance Fund, data from health cards, invoices on issued medicines and medical interventions, the Pension and Invalidity Insurance Fund, records of pension insurers, banks since, in addition to a comprehensive database of their clients, they also have particularly sensitive health data that they collect when deciding on credit claims. There is a great danger of misusing these data and violating individual's privacy.

The Ministry of Internal Affairs established a unit for combating cybercrime, within the Department for Combating Organized Crime at the Police Directorate for Criminal Investigation. This unit cooperates with other organizational units within the Department for Combating Organized Crime, especially with the unit for collection and processing of digital evidence within the Department for Special Investigative Methods, as well as with other organizational units of the Police Directorate and individual security services (SIA, MSA) of the Republic of Serbia. Under the Council of Europe Convention on Cybercrime, cooperation has been established with the

criminal investigation services in other countries for detecting, tracking and preventing the organizations and individuals who commit criminal offenses of cyber crime. Given the fact that cybercrime has a transnational character, cooperation has also been established by the INTERPOL National Central Bureau in Belgrade.

Technical resources and the level of technical and technological structure in a society also affect the safety on the Internet and social networks (Vilić, 2017). Therefore, one of the significant problems in tracing the crimes of cyber identity theft is inadequate technical equipment and insufficient knowledge of the functioning of the high-tech devices operating on the principles of computer systems and networks, as well as modern telecommunication technologies.

Competent police and judicial authorities encounter problems concerning inadequate equipment and staff training, which makes it hard to effectively and properly implement the legal powers entrusted to them concerning the prevention and repression of cyber crime, including the identity theft; these problems also have a great impact on creating favorable conditions for criminal activity related to the use of the Internet and social networks. In this context, it is necessary to consider the lack of a sufficiently effective system of monitoring the Internet, aimed at detecting computer-related crimes, as well as to establish an efficient platform for reporting these offenses, especially at international level. In the process of monitoring, interception, collecting and analyzing messages in the investigation proceedings, it is essential to strike the right balance between the interests of personal privacy and the societal interest in prosecuting the offender.

Conclusion

Although is difficult to define it, identity theft in cyberspace could be defined for the purpose of this paper as a set of criminal actions consisting of the misuse of personal data, the use of another's identity and the violation of the privacy on the Internet and within social network users, as a method for obtaining financial gain, loans and other financial benefits based on fraud and misuse of other’s personal data, or by the taking over of another person's identity for the purpose of inflicting non-pecuniary damage. Considered as such, the identity theft in cyberspace can be treated as part of computer crime in a broader sense. There are various means and methods of identity theft, the most common are phishing (identity theft via e-mail), pharminig (identity theft through malicious software), spear phishing and scam.

A small number of countries in the world have criminal laws that specifically criminalize identity theft in cyberspace, while most of the countries relate identity theft to privacy violations and sanction it as part of the unauthorized collection and use of personal data, unauthorized publishing

and displaying of photographs, illegal access to data, fraud, forgery, copyright infringement, or as acts that precede the commission of another criminal offense. Most of the criminal legislations does not define and sanction identity theft and its forms as a separate criminal offense, but considers it as one of the forms of misuse of personal data.

In order to reduce the number of computer system abuses and privacy violations of the users by identity theft, it is necessary to create appropriate legal mechanisms and regulations for the detection and sanctioning of such socially unacceptable criminal behavior. It is also very important that criminal offenses of computer crime and identity theft are reported to the competent authorities, in order to reduce the "dark crime rate" and to achieve better preventive action, recognition and monitoring of such acts.

References

12th UN Congress on Crime Prevention and Criminal Justice. (n.d.) Retrieved January 31, 2019 from https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

Abdul Manap, N., Abdul Rahim, A. & Taji, H. (2015). Cyberspace Identity Theft: The Conceptual Framework. Mediterranean Journal of Social Sciences 6(4), 594 - 605

All About Phishing (n.d.) Posted March 31, 2006. Retrieved February 26, 2019 from http://www.webopedia.com/DidYouKnow/Internet/2005/phishing.asp

Beal, V. (2016). How to Defend Yourself Against Identity Theft. Retrieved March 13, 2019 from http://www.webopedia.com/DidYouKnow/Internet/2006/identity_theft.asp

Bidwell, T. (2002). Hack Proofing Your Identity in the Information Age. Syngress Publishing, Inc,

Canadian Department of Justice (n.d.). Retrieved February 05, 2018 from http://canada.justice.gc.ca/en/news/nr/2007/doc_32178.html

Cybercrime Convention Comitee – T-CY Guidance Note #4, Identity theft and phishing in relation to fraud, Council of Europe, 2013 (n.d.) Retrieved January 20, 2017 from https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7096

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks (The Facebook Case). Proceedings of the 2005 ACM workshop on Privacy in the electronic society. Retrieved February 02,

2018 from http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf , 71-80

Identity Theft and Assumption Deterrence Act (1998). U.S. Public Law 105-318, Retrieved February 20, 2019 from https://www.ftc.gov/node/119459

Internet Identity Theft (n.d.). Retrieved September 17, 2012 from http://articles.winferno.com/computer-fraud/internet-identity-theft

Ivanović, Z., Uljanov, S. & Urošević, V. (2012). Analiza fenomena krađe identiteta. Zbornik radova, međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na visokotehnološki kriminal, Laktaši 28-30.03.2012., 143-156

Krivični zakonik Republike Srbije. Službeni glasnik Republike Srbije no.85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 and 94/2016

Milićević, S. & Vujović, S. (2012). Problem savremene dobi: oblici krađe i zloupotrebe identiteta i mjere prevencije. Zbornik radova, međunarodna naučnostručna konferencija, Suzbijanje kriminala i evropske integracije s osvrtom na viskotehnološki kriminal, Laktaši 28-30.03.2012., 303-316

Milošević, M. & Urošević, V. (2009). Krađa identiteta zloupotrebom informacionih tehnologija. Bezbednost u postmodernom ambijentu, Zbornik radova knjiga VI, Centar za strateška istraživanja nacionalne bezbednosti, Beograd, 53 – 64

Newman, G.R. & McNally, M.M. (2005) Identity Theft Literature Review. Retrieved February 14, 2019 from https://www.ncjrs.gov/pdffiles1/nij/grants/210459.pdf

OECD Ministerial meeting on the future of the internet economy – Scoping paper on Online Identity Theft, Ministerial background report: DSTI/CP (2007)3/FINAL. (n.d.) Retrieved November 10, 2017 from http://www.oecd.org/sti/40644196.pdf

Out-Law news: „Phishing kits banned by new Fraud Act“ (n.d.). Retrieved March 14, 2019 from http://www.out-law.com/page-7469

Paget, F. (2007). Identity theft. McAfee Avert Labs technical white paper No 1.. Retrieved February 02, 2018 from http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf

Pontell, H.N. (2009) Identity theft: Bounded rationality, research, and policy, Criminology & Public Policy, 8/2, 263-270

Prlja, D. & Reljanović, M. (2009). Visokotehnološki kriminal – uporedna iskustva. Strani pravni život 3 (09), Beograd

Prlja, D., Ivanović, Z. & Reljanović, M. (2011) Krivična dela visokotehnološkog kriminala. Institut za uporedno pravo, Beograd

Roberts, L. (2008). Cyber-Victimisation in Australia:Extent, Impact on Individuals and Responses, Retrieved March 03, 2019 from https://www.researchgate.net/publication/236319661_Cyber-victimisation_in_Australia_Extent_impact_on_individuals_and_responses

Robinson, N., Graux, H., Parrilli, D.M., Klautzer, L. & Valeri, L. (2011) Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime – Final report TR-982-EC. Retrieved January 31, 2019 from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/rand_study_tr-982-ec_en.pdf

Sophos (n.d.). Retrieved January 24, 2019 from http://www.sophos.com/blogs/duck/g/2009/12/14/facebook-privacy-video/

Spear phishing (n.d.). Retrieved March 18, 2019 from https://searchsecurity.techtarget.com/definition/spear-phishing

The Third Interpol Symposium on International Fraud – December 1979 (n.d.). Retrieved August 12, 2017 from http://cybercrimelaw.net/documents/Strasbourg.pdf

The UK Fraud Act (2006). Retrieved February 20, 20119 from http://www.legislation.gov.uk/ukpga/2006/35/pdfs/ukpga_20060035_en.pdf

United Nations Office for Disarmament Affairs – UNODA (n.d.). Retrieved March 12, 2019 from<https://www.un.org/disarmament

United Nations Office of Drugs and Crime – UNODC (n.d.). Retrieved on December 15, 2016 from http://www.undoc.org/

Vilić, V. & Radenković, I. (2015). Pravo na privatnost u svetlu Zakona o zaštiti podataka o ličnosti, XXVIII Kopaonička škola prirodnog prava 2015 - Pravni život 10/2015 LXIV, book 576, 331-341

Vilić, V. & Radenković, I. (2016). Possibilities of Protecting Personal Data Published on Social Network Sites in the Light of the Law on Personal Data Protection, Sinteza 2016 - International Scientific Conference on ICT and E-Business Related Research, Belgrade, Singidunum University, Serbia, 62-65, DOI 10.15308/Sinteza-2016-66-73

Vilić, V. (2017). CYBERCRIME: Basic criminological characteristics and legislation. LAP - LAMBERT Academic Publishing – International Book Market Service Ltd.member of OmniScriptum Publishing Group. -166. ISBN 978-620-2-01800-5

Zakon o zaštiti podataka o ličnosti. Službeni glasnik RS no. 97/2008, 104/2009 - dr. zakon, 68/2012 - odluka US, 107/2012