UNIVERSITY OF MARIBOR
FACULTY OF CRIMINAL JUSTICE AND SECURITY

POLICING IN CENTRAL AND EASTERN EUROPE – SOCIAL CONTROL OF UNCONVENTIONAL DEVIANCE

CONFERENCE PROCEEDINGS

Editors
Gorazd Meško, Andrej Sotlar and John Winterdyk

LJUBLJANA, 2011

Proceedings of the conference
"Policing in Central and Eastern Europe – Social Control of Unconventional Deviance",

Ljubljana, Slovenia
22-24 September 2010

Editors: Gorazd Meško, Andrej Sotlar and John Winterdyk
Technical editing: Maja Jere
Printed by: Tipografija d.o.o.
Threshold: Tipografija d.o.o.
Drawings: Philip Spence, Fellow of the Wolfson College, Cambridge, UK.
Cover page design: Tipografija d.o.o.
Printed: 500 copies

CIP - Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

343.85(4-191.2-11)(082)

POLICING in central and eastern Europe - social control of unconventional deviance : conference proceedings, [Ljubljana, Slovenia, 22-24 September 2010] / editors Gorazd Meško, Andrej Sotlar and John Winterdyk ; [drawings Philip Spence]. - Ljubljana : Faculty of Criminal Justice and Security, 2011

ISBN 978-961-6821-10-0
1. Meško, Gorazd
256486912

This publication was published by the Faculty of Criminal Justice and Security (FCJS), University of Maribor, Kotnikova 8, 1000 Ljubljana, Slovenia in June 2011 and arises out of the eighth biennial conference Policing in Central and Eastern Europe held in September 2010 at the FCJS (www.fvv.uni-mb.si/conf2010). This publication consists of peer reviewed conference papers only. These conference proceedings are included in the Conference Proceedings Social Science Citation Index (Thomson Reuters).
The editors are grateful to all authors for their contributions to this publication and peer reviewers for their valuable contributions to the improvement of draft papers.
The conference Policing in Central and Eastern Europe – Social Control of Unconventional Deviance (2010) was financially supported by the National Research Agency of the Republic of Slovenia (Grant No. 6304-87/2010-1).

Table of Contents

PHISHING SCHEMES – TYPOLOGY AND ANALYSIS IN SERBIAN CYBER SPACE

Authors:
Božidar Banović, Vladimir Urošević and Zvonimir Ivanović

ABSTRACT

Purpose:
The purpose of this paper is to identify and describe various factors for understanding criminal behaviour involved in phishing and to provide advice – in the areas of security, criminal procedure, and victimology.

Design/methodology/approach:
The project combined several qualitative and quantitative techniques such as interviews and surveys, as well as content analysis.

Findings:
Several categories of subjects were identified: those who are aware of some scientific achievements in this field and who feel increasingly apprehensive about the disclosure of private information; those who are not prepared to readily incorporate scientific progress in similar fields; the third category includes staff members who do not embrace all new measures in the fight against this type of cybercrime. The participants could also be categorized on the basis of their inclination to recognize new forms and types of phishing: some are aware of new forms and can recognize them as soon as they emerge locally; others cannot do so.

Research limitations/implications:
To allow findings to be generalized, future research should include measures that could specify additional means to be used by members of a wider representative group, such as tools, materials, educational and course modules, implemented during training.

Practical implications:
This research represents a useful source of information for method implication in combating phishing schemes, and for detecting new emerging forms and types of cybercrime promptly, as well as new social engineering methods to facilitate it.

Originality/value:
This paper should be of particular interest to forensic specialists, in the analysis of crime scene behaviour and of methods phishers use in luring their victims.

Keywords: Phishing, Spear Phishing, Pharming, Cybercrime

1 INTRODUCTION

Phishing schemes (The term term was first used by Gercke, Đokić, Radulović, Petrović, Lazović & Prah (2008:147) and in Nikolić, Gvozdenović, Radulović, Milosavljević, Jerković, Živković, Živanović, Reljanović, & Aleksić. (2010:30), in Serbian literature, and in the world term was first used in 1996. according to Jakobsson & Myers (2007:3)) are currently the most prevalent manifestations of cybercrime phenomena. Types and phenomenology of this type of crime are evolving on a daily basis, as does the sophistication of its perpetrators, so research in this area is extremely important. The importance of such research lies in the phenomenological mapping of manifested forms in order to solve crimes in the area. This paper aims to create a map of the present state of affairs of this area in Serbia. Focal groups are experts who deal with cybercrime, especially electronic crime. The aim of the research is to present the characteristics, variations, and interdependence of various elements in phishing and spear phishing schemes. The most secure way to achieve this was to investigate specific expert knowledge and judgements in this area by means of surveys and interviews.

2 THE SURVEY

The key objectives of this study were:

To examine phishers' behaviour, MO, and signatures from expert points of view; to understand the relationship between victims' actions, their jobs, current positions, and connected jurisdictions; to discover how and why perpetrators find, lure, and catch specific victims; and to find out what perpetrators do with the obtained personal data, thereby mapping the route and destination of such stolen data.

2.1 Sample and methodology

The total sample includes 20 experts in four different fields: the judiciary, bank security personnel, the police, and the public prosecutor's office. Their expertise lies in the field of cybercrime but in separate areas. This fact helped us acquire more precise study results.

Interviews and surveys were conducted on the same day in June 2010. Each survey lasted for 10 minutes while each interview lasted for 15.

In reviewing this report, please note that percentages may vary or did not add up to 100 %, due to rounding, the existence of multiple answers to one or more questions, or the exclusion of any "not sure" or "decline to answer" responses.

This initial research implemented Delphi research methods; during the interview participants were introduced to the dispersal of answer percentages so that they

could predict answers to the interview questions more precisely. It was conducted among attendants of the "Credit and debit cards in 2010"conference held in Belgrade, and organized by the Serbian Chamber of Commerce. Participants were from different sectors, such as bank e-security, the police hi-tech crime unit, judges, and public prosecutors specialized in e-crimes. The number of survey participants was twenty (n=20). Each participant was asked to take an anonymous survey, with a brief description of its content, goals and methods used. Everyone was asked not to give or disclose any personal information and was informed that, if anybody did, that information would be lost in the process. If they wished to see the results of this survey l participants were asked to contact its organizers of by mail; they would get a copy of the results and analysis upon its completion. Researchers explained in the addendum to the survey that any participant was free to give more than one answer, and where possible, to give a different answer from that given in the survey, specific to the participant. The participants were informed about the aims and goals of the survey and broader research project of phishing typology, of which the given surveys and interviews formed part.

3 THE RESULTS AND DISCUSSION

With respect to the question: "Do you consider phishing more dangerous than other forms of cybercrime?" participants of the survey were ambivalent; half considered phishing to be the most dangerous among other forms of cyber crimes, while the other half (i.e. 50 %) thought it not to be as dangerous, or no more dangerous than other cybercrimes (Figure 1).

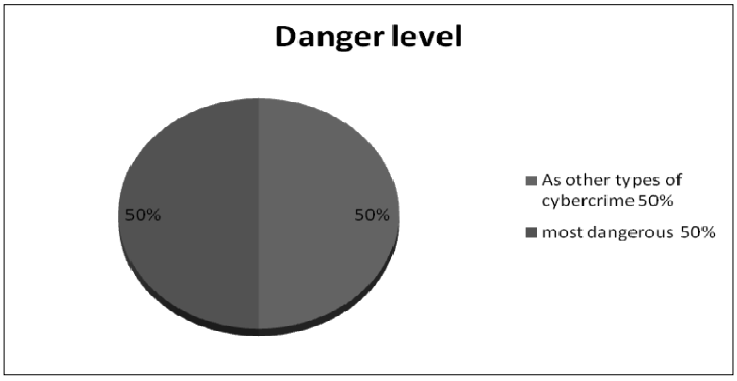

Figure 1: Danger level of the phishing

The reasons for believing phishing to be not so dangerous could be found in the global action to suppress the phishing phenomenon, while the other result was probably due to the real danger of the phenomenon itself (Smith, Grabosky &

Urban, 2004). This result may stem from awareness-raising campaigns against phishing in Serbia, focusing on the banking sector, together with action against and strategic preparedness for this and other types of cybercrime. Regarding the behaviour of perpetrators, this could mean that participants are not very focused on behavioural analysis, but much more interested in the phenomenology of the issue. In analyzing their responses, we could distinguish two types of participants: those who underestimated the phishing issue, and those who did not.

With respect to another question regarding what types of phishing were most common in their everyday life, 92.3 % of all survey participants replied that the most common phishing schemes were in English language, and only 7.7 % thought that they were in Serbian (Figure 2).

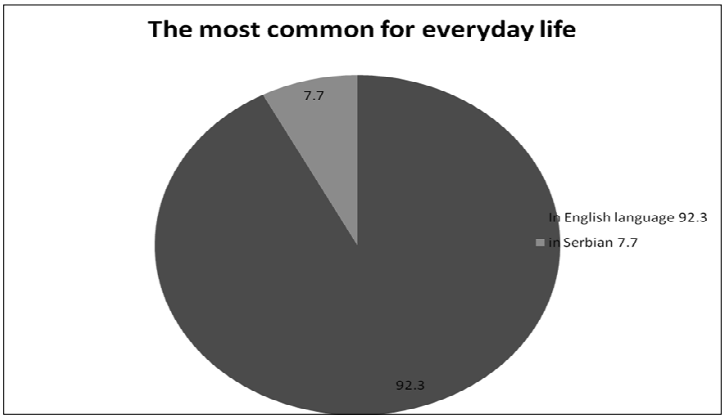

Figure 2: The most common phish for everyday life

This question and answers to it revealed for the first time the presence of phishing schemes in poor Serbian language in this geographical area. This could mean that perpetrators tend to cover this geographical area, because of its significance in terms of economic resources but also because of its potential role in spreading the business of organized criminal groups in this area. One explanation could be the use of PoC honeybots or other automated bot systems, and online free translation tools such as Google Translate or others, to socially engineer their scheme. This result could also be read as a victimology analysis, where the targeted victims were not just English-speaking people in Serbia, but also Serbian victims not speaking English language. This is very alarming, and provides valuable feedback for the phishing campaign, especially regarding awareness of Serbian language (poorly crafted, but fully functional) phishing schemes in this area. The dissemination of answers, with the vast majority confirming English language phishing schemes, still confirms the perpetrators' tendency to use mass mailing and bot systems, rather than focused attacks, such as spear phishing. But the other group certainly revealed the existence of such attempts in this area.

Most participants distinguished spear phishing (83.3 % of all answers) from common phishing scheme, but nevertheless 16.7 % of participants considered the two to be the same (Figure 3).

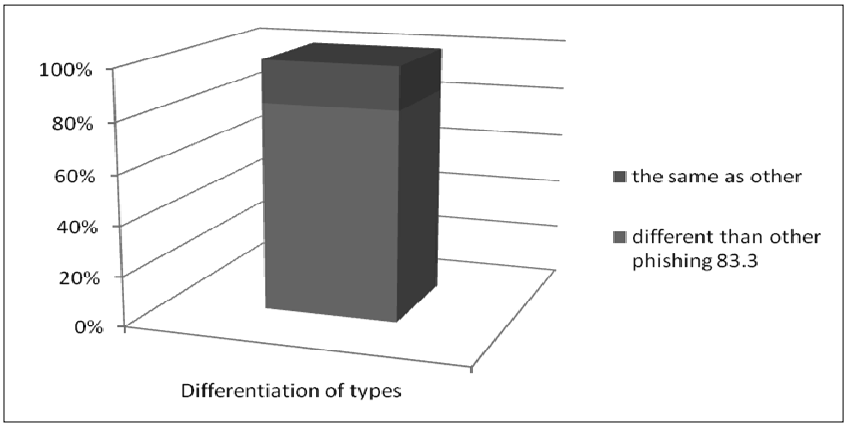

Figure 3: Differentiation of phishing types

Again, this could be interpreted as resulting from anti-phishing campaigns, but could stem from existing daily phenomena in business life in Serbia: phishing mail, targeting CEOs and other high ranking officials in well-led businesses as well as state officials.

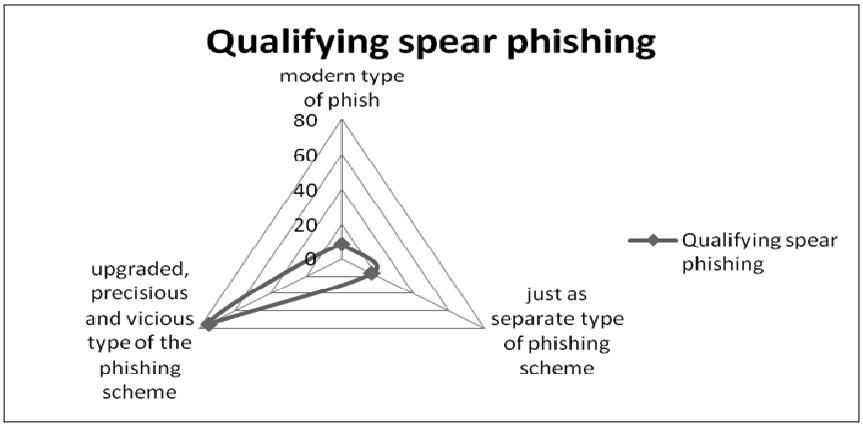

Figure 4: Qualifying spear phishing

This question alone indicated the existence of spear phishing and its possible implications in Serbian cyberspace. One could deduce that this area is therefore no exception, and that soon spear phishing mails may result in successful fraud, resulting in CEOs and other officials giving away valuable professional and private, even personal, information to phishers. One can speculate that, with poorly crafted phishing schemes in Serbian language – probably made with bots and DDoS

attack engines, organized, educated expert perpetrators could craft very attractive spear phishing schemes aimed at higher CEOs and other VIPs, which could result in acquiring everything – from digital IDs to well-kept company secrets.

The question: "do you consider spear phishing to be a modern type of phishing?" resulted in 8.3% affirmative answers, while 16.7 % did not consider it to be a modern variation, but just a separate type of phishing scheme. The vast majority (75 % of all participants) considered spear phishing to be an upgraded, precise and vicious type of phishing (Figure 4). This result could be due to massive bulk mail attacks, present in Serbian cyberspace, most prominently in the banking sector, from which the majority of participants came. This also answer the question of which sector is most vulnerable to this type of attack, although the diversity of answers also indicates a wrong understanding of the phishing phenomenon itself. Just 10% of participants did not distinguish between spear phishing and classic phishing, while the remaining 90% had different specializations in categorizing its modern elements.

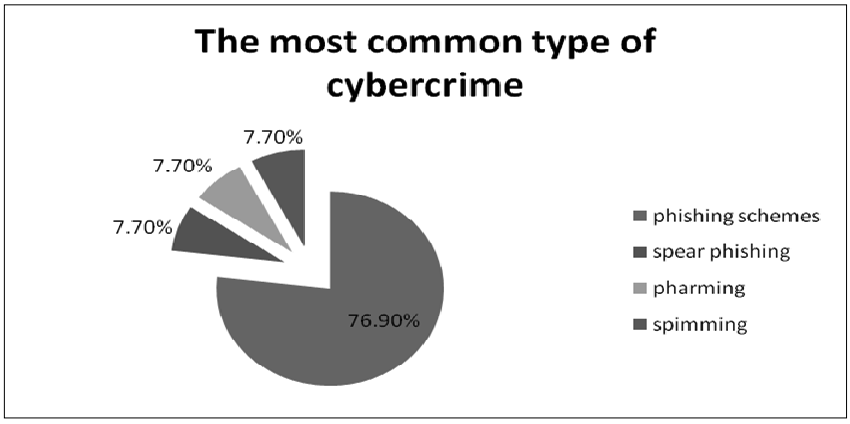

Figure 5: The most common type of cybercrime

The most common type of cybercrime, present in common business life and encountered by cybercrime law enforcement agencies in Serbia, involves phishing schemes, as stated in 76.9 % of participants' answers. This is followed by spear phishing, pharming, and spimming, each accounting for 7.7 % (Figure 5). Although this also revealed the existence of pharming and spimming attacks in Serbian cyberspace, the overall result very accurately positioned the existing and growing problems of phishing and spear phishing. All of this indicates that future strategic, tactical, and operational measures should be taken by the government and policy makers. Of course there must be deeper thorough scientific research in this area before any action is taken in the field, but hopefully this research could give some guidelines for future research. The most interesting fact is that Serbian legislation does not actually specify incriminating acts that would cover activities like phishing and spear phishing, pharming or spimming.

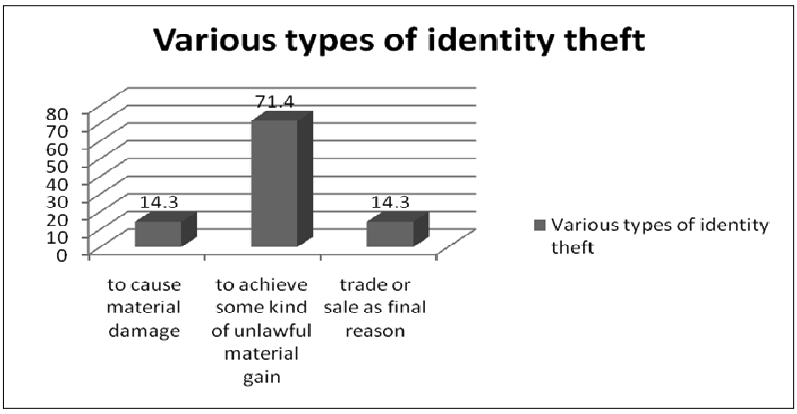

Figure 6: Various types of identity theft

The participants considered various types of identity theft (even virtual identity theft) intended to cause material damage to somebody (14.3 % of all answers) or to obtain some kind of unlawful material gain for the perpetrators or others (71.4 % of all answers), or finally having trade or sale as the ultimate motive for the ID theft (14.3 % of participants) (Figure 6). One could argue that in a country that has not incriminated ID theft offenders there are serious implications. Nevertheless all survey participants confirm that there must be some knowledge about the phenomenology of ID theft, its motivation, and outer manifestations. This is therefore an opportune time for the analysis of phishing and other types of ID theft within Serbian cyberspace.

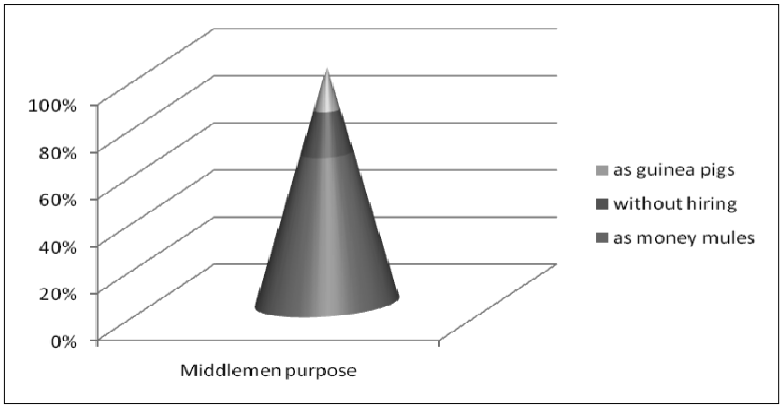

Figure 7: Purpose of middlemen

Another question was: "Is it possible, according to your knowledge, that perpetrators often hire middlemen in the perpetration and realization of such crimes?" Here a large percentage of participants, 63.6 %, responded that perpetrators do hire fraudulent collaborators (Petrović, 2004) as money mules to handle money or goods gained through phishing; 18.2 % of the participants

did not perceive perpetrators as an organized group of men or women, but as solitary 'gunmen' acting alone. Another 18.2 % of participants perceived perpetrators as people using other people as guinea pigs for their quests (Figure 7). The vast majority of answers (81.8 %) showed that all of these acts contain a common element involving systematization, implicating the existence of organized crime in this area.

The responses to our next question required engaging the professional and personal experience of the participants. We found that 7.7% regarded phishing schemes as too naive, poorly crafted fishing hooks, which could not lure a real fish, and therefore not a real phishing victim; 23.1 % of the participants found them relatively naive judging by their general and overall characteristics; 15.4 % found them subtly perfidious, while the vast majority (46.3 %) thought them extremely dangerous, especially spear phishing schemes (Figure 8).This result could be due to real danger arising from phishing and spear phishing (according to the largest group) but there still appears to be a significant percentage of survey participants who underestimate this phenomenon in Serbian cyberspace. Surprisingly, despite official awareness-raising campaigns, the group who consider phishing to be naive could be influenced by further prevention-awareness campaigns by law enforcement officials. One of the answers was open and referred to the focus group. In the participants' opinion, older citizens were more vulnerable than others, especially since their "pride and experience" are likely to be targeted by the phishers, as well as their naivety concerning URL difference.

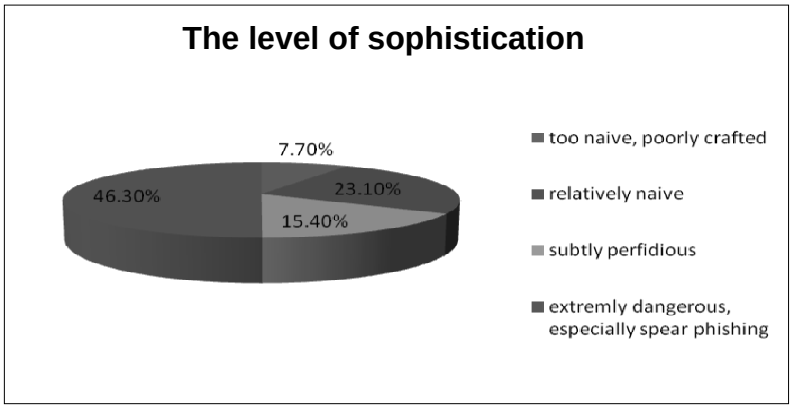

Figure 8: The level of sophistication

The next question was: "Do you consider social networking as a future cyberspace field for the realization of phishers' schemes?" Interestingly, the vast majority of participants (78.6 %) considered it to be ideal for future phishing schemes, and 7.2 % of the participants thought that social networking sites already provide a fertile field for phishing schemes.

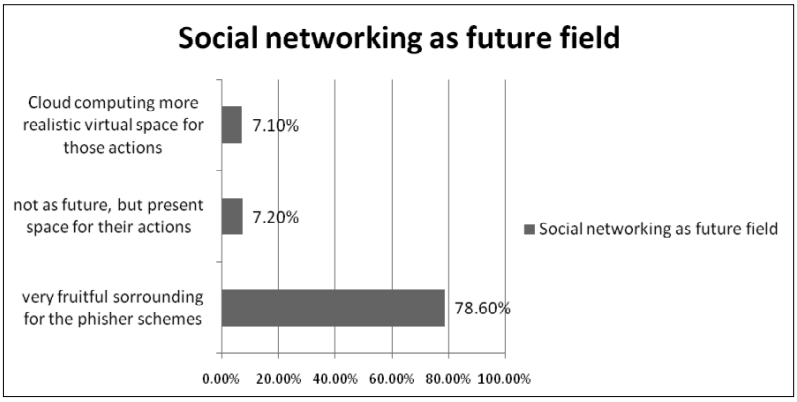

Figure 9: Social networking as future field

A small percentage of participants (7.1 %) found Cloud computing to be more realistic virtual space for phishing and more recent forms of cybercrime (Figure 9). This distribution of results shows that phishers are seriously present in social networking today, but that more danger comes from contemporary and modern types of computing applications on the web. It also shows that there is very high awareness of fraud problems in Serbian cyberspace among bank and police personnel

The last question showed that participants (84.6 %) regarded bank clients as the most vulnerable group with respect to phishing attacks. CEOs of banks and business firms were regarded as targets by 7.7 % of participants, while 7.7 % thought that the target group comprised uneducated persons with important positions in the state i.e. those not familiar with fraudulent online trade, gaining personal and other data for ID theft (Figure 10).

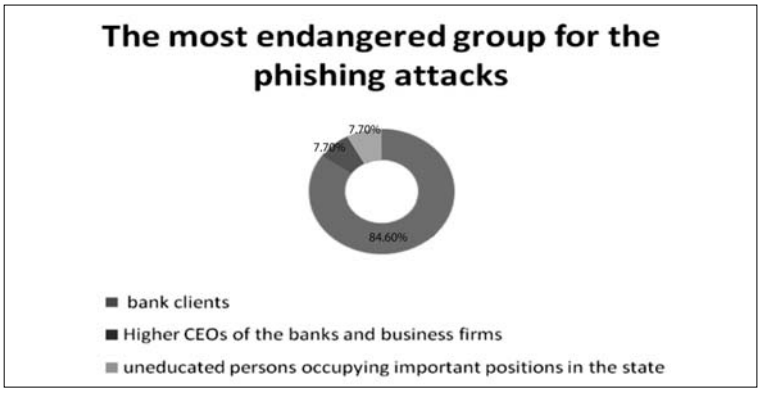

Figure 10: The most endangered group for the phishing attacks

Besides the survey questionnaire, some participants were also interviewed so as to address the problem in depth, in order to create a model to explore the phenomenon of phishing. In the course of informal conversation, experts were

asked their opinions and shared their experiences in the field, in order to create a practical and useful model. In all interviews, ignorance and a false belief in the security policy of their institution combined with a misplaced feeling of full security was identified: the minority of participants were aware of some scientific achievements in this field, with growing fear of breaches of private information in any field; the vast majority felt confident about their security capabilities and the legal apparatus to deal with cybercrime issues, and were not prepared to readily incorporate scientific progress in similar fields; one section of the interviewed group were employees who did not readily embrace all new measures in fighting this type of cybercrime. Those categories also could be sub-divided according to their recognition of new forms and types of phishing schemes. Thus we can recognize those who are aware of new forms and can recognize them as soon as they emerge locally, and those who cannot. From the interviews we were able to identify answers which could be used to design a cybercrime prevention model, also to safeguard bank security. These were "security tips" (something similar can be found at Касперски, 2001, p.5) relevant for business mailing systems, with rules of behaviour for employees in circumstances targeted by phishers. Some valuable answers were also acquired for mobile telephone and IM usage. There were answers combining social networking with previously covered fields (IM, mobile, prevention in banking). The combined results of the survey and interviews prove very useful for wide-ranging possible implementation, from mobile telephones and computing, to social networking and even cloud computing. This is presented in the following figure.

The following characteristics of ID theft can be identified. Two steps are 'simple': acquiring the data and storing it. Those activities are the most sophisticated and constantly evolving, and therefore the most difficult to stop. We can therefore focus on the motives lying beneath those acts: from the results of our research we recognize the following. Firstly, personal use of the data by the perpetrator is the rarest of all types. Here we could recognize the perpetrators' attempts at covering their tracks by engaging money mules to do dirty jobs for them. The engagement of a middleman ranges from withdrawal of cash from the victim's bank account and online shopping, to concluding transactions in favour of third parties. The second motive lies in further commercial use of the obtained data, also engaging a middleman (money mule) but this time in favour of a third party, not present in the deal. The data will typically be chopped to pieces and sold bit-by-bit, since the ID consists of several elements, all of which can be used and sold separately. Here we recognize gain in favour of a third party and for the benefit of the perpetrators themselves directly in their bank accounts. The third motive lies in creating the possibility for further trade from the data acquired, but not all at once. The fourth motive could be defined as causing damage to other persons.

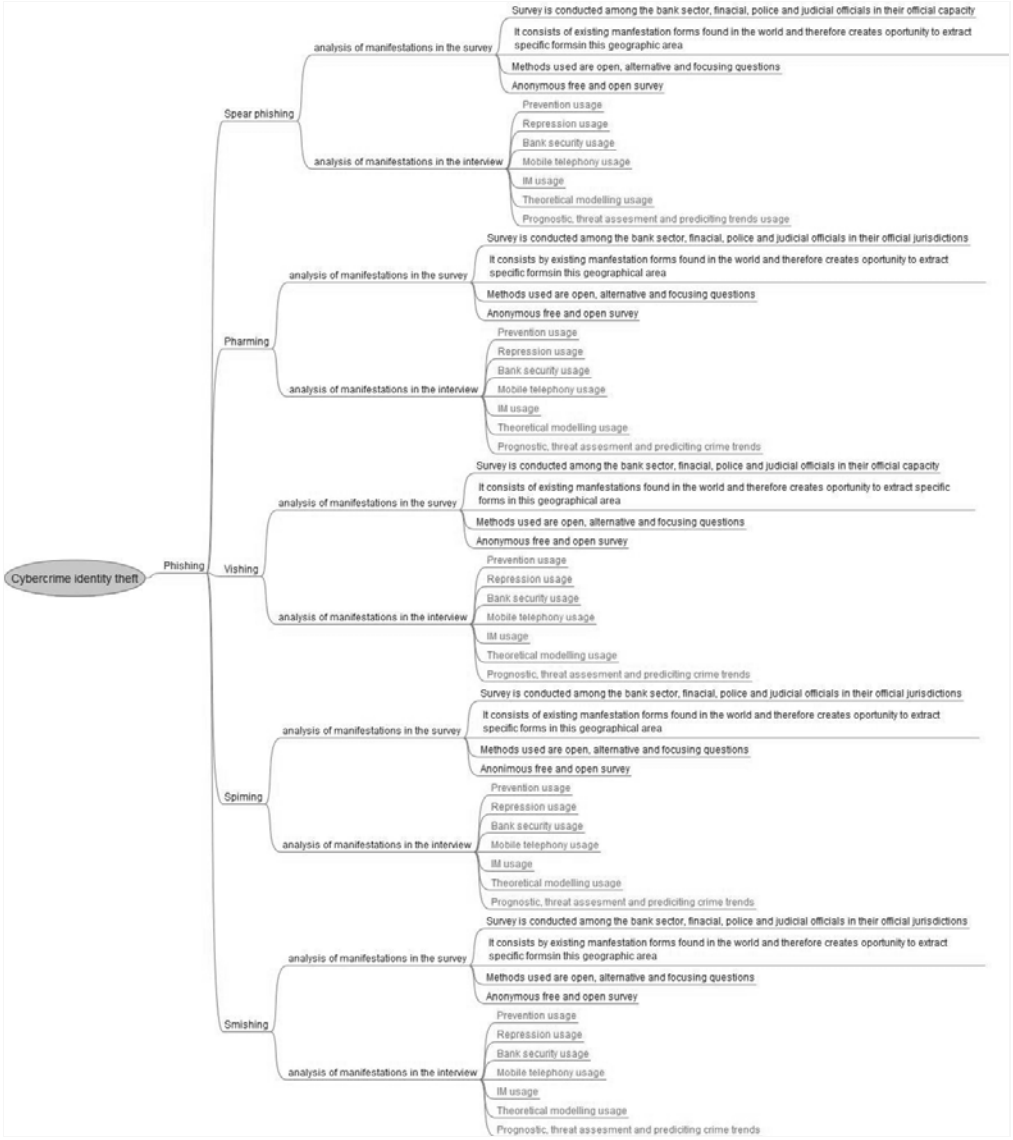

Figure 11: Phishing attack vectors

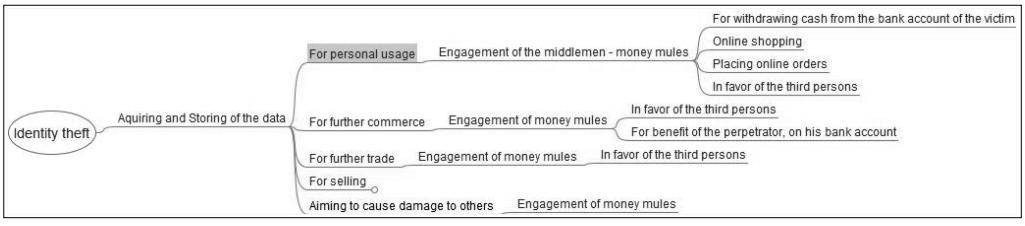

Figure 12: Motives for acquiring and storing the data

4 CONCLUSION

This paper presents a useful source of information for methods to suppress phishing schemes. It explains new forms of cybercrime, with its ever-emerging new types and modes, as well as new methods in the social engineering facilitating it. The understanding of cybercrime among staff in charge of processing crime scene evidence, especially among the police, bank and other financial organizations' personnel, should be of particular interest to forensic specialists in their attempts to analyze crime scene behaviour, and the methods used by phishers in luring their victims.

Based on the results obtained in this research, one can visualize the present situation in Serbia. Various elements of phishing and spear phishing schemes, their interdependence, as well as their different manifestation were provided through the exploration of expert knowledge and judgement in this specific area from a wide range of different sectors, such as bank e-security, the police hi-tech crime unit, as well as judges and public prosecutors specializing in the field of e-crime.

The results of these interviews clearly indicate that, as far as the behaviour of perpetrators is concerned, participants were not so focused on behavioural analysis, as they were on the phenomenology of the issue. Analysis indicates that we can find two types of participants: those who underestimate phishing issues, and those who do not. The vast majority of phishing attacks are conducted in English language but it is an alarming fact that there are also attacks in the Serbian language. The most valuable finding was the existence of spear phishing. One can speculate that with the presence of poorly crafted phishing schemes in Serbian language (probably made with bots and DDoS attack engines) well-educated, organized, expert perpetrators could craft attractive spear phishing schemes aimed at higher CEOs and other VIPs. These schemes could result in various thefts – from digital IDs to well-kept company secrets.

Only 10% of participants did not distinguish spear phishing from classic phishing, while the others have different specializations in categorizing modern phishing elements. The existence of pharming and spimming attacks in Serbian cyberspace was very accurately defined as a current and rapidly growing problem, alongside phishing and spear phishing. All this could be indicative for future strategic, tactical, and operational measures by the government and policy makers. Of course, there must be deeper and thoroughly scientific research in this area before taking any actions in the field, but hopefully this research could give some guidelines for future research. The most interesting fact is that Serbian legislation does not yet specify incriminating acts to cover acts like phishing, spear phishing, pharming or spimming (although the last criminal phenomenon could theoretically be legally defined as attempted fraud, punishable under Section

208 of the Criminal Law of the Republic of Serbia although not strictly defined as crime *per se*).

One could argue that in a country that has not yet incriminated ID theft (solely or as part of phishing crime) we have to consider the implications of this criminal act very seriously. All research participants suggest that there is awareness of ID theft, its motivation, and outer manifestations. The research presented shows that this is a new moment for anybody analyzing phishing and other types of ID theft in the Serbian cyberspace.

One simple fact shows that a vast majority of the participants (78.6 %) consider social networks to be very fruitful surroundings for phishers\ schemes, but 7.2 % of the participants find it not as a future, but rather a present space for their actions. There are 7.1 % of the participants who find Cloud computing to be a more realistic virtual space for those actions and more recent cybercrime forms. This distribution of survey results shows that the phishers are very seriously present in social networking today, but that there are more dangers coming from contemporary computing applications on the web[1]. It also showed that there is a very high level of awareness of fraud-related problems in the Serbian cyberspace among bank and police staff. The most endangered group for the phishing attacks, as perceived by the percentage of 84.6 % subjects, are bank clients. Higher CEOs of the banks and businesses are described as targeted by 7.7 % of the participants, and 7.7 % find uneducated persons occupying important positions in the state i.e. those who are not familiar with the functioning of false online trade, aimed at fraudulently gaining personal and other data for ID theft.

Results from open interviews showed that participants could also be divided into categories with respect to their inclination to recognize new forms and types of phishing schemes and that here we can see those who are aware of the new forms and can recognize them as soon as they emerge locally, and those who cannot.

In recapitulation, we can underline some relations found in this research, between: the victims' actions and luring methodology, targeted assets and their later use by perpetrators or money mules, defensive actions taken by victim, their work position and type of phish, surroundings, the victim`s education and type of phish, complexity of the phishing scheme and targets, organized crime and realization of phishing schemes.

Phishing and spear phishing are emerging trends in cybercrime in the territory of the Republic of Serbia. Most groups that are endangered by this type of cyberattacks have some relevant experience in reporting on such activities and their prevention, but raising awareness and research studies like this one, conducted

[1] For comparison, look into Athanasopoulos, Makridakis, Antonatos, Antoniades, Ioannidis, Anagnostakis, & Markatos, (2008).

among bank e-security, police hi-tech crime unit, judges and public prosecutors from the specialized area of e-crime are the best way to describe the present situation and to point out what future trends and arising problems in this field are. International cooperation in suppressing cybercrime is of great importance. More about this topic can be found in the works of Portnoy and colleagues (Portnoy & Goodman, 2009), and Xingan (Xingan, 2010).

REFERENCES

Abad, C. (2005). *The economy of phishing: A survey of the operations of the phishing market*. San Francisco; Singapore; London: Cloudmark.

Athanasopoulos, E., Makridakis A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K. G., & Markatos, E. P. (2008). *Antisocial Networks: Turning a Social Network into a Botnet*, Section: Network Security, Lecture Notes In Computer Science. Retrieved from http://www.ics.forth.gr/dcs/Activities/papers/facebot.isc08.pdf

Dragoon, A. (2004). *Foiling phishing*. CSO Online.

Gercke, M., Đokić, D., Radulović, S., Petrović Z., Lazović, V., & Prah, R. (2008). *Priručnik za istragu krivičnih dela u oblasti visokotehnološkog kriminala*. Savet Evrope.

Jakobsson M., Myers S. (2007). *Phishing and Countermeasures Understanding the Increasing Problem of Electronic Identity Theft*. Hoboken; New Jersey: John Wiley & Sons, Inc.

Касперски, К.(2001). *Техника сетевых атак*. Издательский дом "Солон-Пресс".

Nikolić, L. K., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Reljanović, M., & Aleksić I. (2010). *Suzbijanje viskotehnološkog kriminala*. Beograd: Udruženje javnih tužilaca i zamenika javnih tužilaca, AECID.

Petrović, S. (2004). Kompjuterski kriminal. Beograd: Vojnoizdavački zavod.

Portnoy, M., & Goodman, S. (2009). *Global Initiatives to Secure Cyberspace an Emerging Landscape*. Springer Science + Business Media, LLC.

Rapetto, U. (2006) Transnational Crime: Challenges for Law Enforcement. In U. Gori & I. Paparela (eds.), *NATO Security through Science Series - E: Human and Societal Dynamics* (pp. 63-66). Invisible Threats: Financial and Information Technology Crimes and National Security.

Smith, R. G., Grabosky, P. N., & Urban, G. F. (2004). *Cyber criminals on trial, defining and measuring cyber crime*. Cambridge; New York: Cambridge University Press.

Xingan L. (2007). International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene. Webology 3/2007. Retrieved January 2, 2010, from http://www.webology.ir/2007/v4n3/a45.html.