Analysis of phishing attacks against students

Jakov Andrić*, Dijana Oreški**, Tonimir Kišasondi***
* NTH, Varaždin, Croatia
** Faculty of Organization and Informatics, Varaždin, Croatia
*** Open Systems and Security Laboratory, Faculty of Organization and Informatics, Varaždin, Croatia
andric.jakov@hotmail.com ; dijana.oreski@foi.hr ; tonimir.kisasondi@foi.hr

Abstract - Aim of this research was to examine familiarity of students in Croatia with threats in form of social engineering and phishing attacks. To obtain our research data, a practical assessment of student's capabilities to identify phishing attacks against them was conducted with the help of a graphical questionnaire that presented real phishing messages that tried to identify what kind of scams or attacks were successful against students and what security topics are needed to identify and protect against phishing attempts. This paper shows the result of our work, some thoughts on phishing research and the identified features that are problematic for students' detection of phishing and social engineering attacks.

1. INTRODUCTION

One of the more pressing issues in computer security are targeted attacks against users with the help of methods that rely on social engineering to have an effect against their targets, where that effect is usually an attempt to collect sensitive information like access data for certain systems [1]. Social engineering attacks exploit the inherit trust that people have in communication, since an average computer user that is not trained to identify social engineering attacks will most likely be a victim to such targeted attacks.

Depending on their level of sophistication, when we talk about phishing attacks we think about mass scale, non-targeted attacks against multiple individuals in one or more organizations. Such attacks are usually low in sophistication, and can be extremely effective if the user is gullible enough to divulge his username/password combination or any other piece of sensitive data. This usually helps attackers in multiple ways: users usually reuse passwords, so by obtaining one set of credentials, there is a high probability that those credentials will work on multiple services, and the second one is, if the user can be tricked into running a malicious file that contains a trojan or any other type of malware on his computer, attackers can easily pivot their attacks inside the organization.

As with all classes of attacks, attackers usually improve their attacks by gaining familiarity and additional data about a target. Spearphishing attacks refer to the class of attacks where attackers collect additional data about a target usually from public sources or social networks to make sure that they can craft a persuasive e-mail that would increase the chances that a user will divulge sensitive data or execute a file that contains malware. If the target of the attack is a executive who has access to classified or sensitive data in the organization or a system administrator who has administrative access to computer systems where the attack is specifically crafted against a high value target, we call this type of attack whaling (as a reference that the attackers are trying to catch a really big fish) [2, 3, 4].

When we try to estimate the damage that phishing attacks cause, there are multiple interesting cases we can refer. One of the most interesting cases is the recent attack against the bitcoin startup and exchange Bitstamp. Bitstamp is a bitcoin exchange, meaning the users can use Bitstamp to convert between the the digital currency Bitcoin and fiat currency (like euros or dollars). In January 2015, Bitstamps operations were suspended as a part of an investigation of a possible intrusion in Bitstamps systems. The attackers used a series of targeted phishing attacks against multiple employees, where a system administrator opened a malicious attachment in a personalized phishing mail, and infected the machine of the system administrator. With the help of this access, the attackers managed to steal 19.000,00 BTC (bitcoin) with an estimated value of five million USD [6].

2. RELATED WORK

Phishing research is not a novel research branch. There are multiple related papers that cover susceptibility of individuals to phishing attacks where the research area focuses on the question of why do people fall for phishing and what kind of people fall for phishing. Other papers focus on development of methods that enable identification of phishing e-mails with varying amounts of success. The third interesting branch is user education, where there are multiple papers that focus on how to educate users to be more resistant to phishing attacks.

Mohebzada, Zarka, Bhojani and Darwish [7] conducted two large scale phishing experiments on 10.000 individuals that were students, alumni, faculty and staff of the American University of Sharjah in Australia. They did not inform their subjects that they will be a subject in their experiment, but they did obtain the authorization from the Faculty's Ethical board to proceed with their research. Their research concentrated on the demographics of the subjects that fell for phishing attacks where they showed

This work has been supported by the Croatian Science Foundation under the project IP-2014-09-3877.

that there is no strong correlation to demographics and their susceptibility to phishing attacks.

Sheng, Holbrook, Kumaraguru, Cranor and Downs [8] tried to link demographics and phishing vulnerability, where they found that female and younger test subjects are more susceptible to phishing attacks. Dodge, Carver and Ferguson conducted similar studies against military cadets [9] where about 80% of cadets failed to identify phishing messages. A similar research was conducted in Indiana University by Jagatic, Johnson, Jakobsson, and Menczer [8] where the researchers tried customizing their attacks by using information from the research subject's profiles on social media, in this research, their success rate was 72%, which showed that targeting a user with additional data can provide a significant advantage for an attacker.

Sheng, Magnien, Kumaraguru, Acquisti, Cranor, Hong and Nunge [9] successfully implemented gamification concepts to phishing education which they described in their paper "Anti-phishing Phil: the design and evaluation of a game that teaches people not to fall for phish" where they created an online game that educates users about phishing. The game focused on identifying URL's that might be malicious, where verification showed that the game had an effect that the users were more cautious when identifying future phishing attacks. This research gives an idea to "gamify" potential phishing attacks to test users, as we did in our paper.

Wang, Herath, Chen, Vishwanath and Rao [10] researched how people process phishing mails' and found out that reduction of the depth of information processing induces recipients to make errors, in which they fall for phishing attacks which is tied to deception indicators that help subjects recognize deceptive measures. By increasing the subjects' knowledge on deception indicators and how their knowledge about scams their attention is heightened against their visceral triggers on the likelihood to respond.

Other papers have explored automated methods to detect phishing messages, like the use of multi-label rules in associative classification to detect potential phishing messages like in [11] or usage of supervised learning algorithms like multilayer perceptrons, decision tree induction or naïve Bayes classification like in [12] or heuristics like in [13] where there are multiple interesting avenues for phishing research like feature extraction, where extracted features can be used in other experiments and tests.

3. RESEARCH LIMITATIONS

Research into targeted attacks against users that falls into the social engineering class of attacks has a number of interesting issues that can influence the results of such studies. The one area is the legal and ethical issues. Any social engineering attack that collects potentially sensitive or private data with the help of a computer system can fall and usually falls under the area of potential violation of cyber crime laws, since a computer system is used to unlawfully obtain sensitive data without the user's consent. If we want to lawfully conduct phishing attacks against users, we need to either obtain the permission and consent from their organizations management or we need to obtain permission from the users themselves. In case of obtaining the permission form the users, the scientific validity of the testing can be skewed since the users know that they will be tested and they need to correctly identify the attack as malicious. This fails the requirement that all experiments with users should be blind to eliminate any bias with testing. If we obtain the permission from the board or management of an organization as in a case of a penetration test, the management or someone in the authorization or procurement chain can intentionally or unintentionally leak the information that a test will be conducted, where again the test will have a bias if the organization wants to present itself as secure.

If we want to conduct a realistic phishing test, we need to collect sensitive data to realistically show that a user was indeed successfully exploited or "trick" the users into opening a malicious attachment. The collection of sensitive data is a security problem, since when the data is collected, we need to notify the user that the data is compromised, which in the case of usernames and passwords usually means that the user or organization will have to rotate that compromised set of credentials, also when we collect data, there is a possibility of unintended data leaks or that the test credential set can be stolen, leading to a security incident. An additional problem is the fear of reprisal the users might have if their management / executives find out that they failed a security test and they are a weak link in the security chain. This makes testing difficult, since the users are influenced and biased before the test.

The problem of identifying successful attacks in phishing tests is way simpler with a "malicious" attachment where the attachment is not real malware, but "testware" where the crafted testware won't infect the system, but just send a identifying ping or request to the researchers server. The problem with this approach is that it doesn't account for host based security measures that might stop the infection.

The third problem is how should the users react to phishing attacks? If the organization doesn't have an implemented information security management system and doesn't train their employees to detect phishing or social engineering attacks, usually their employees will be far more susceptible to such attacks and will become victims of such attacks. If they do identify the phishing mails correctly, usually users will simply ignore the e-mail because they correctly identified the e-mail as malicious or simply ignored or didn't see that e-mail, which doesn't help us with identifying the exact reason why an attack failed or succeeded. Developed organizations have systems that the users can use to flag phishing e-mails or report them to the security department, which is especially useful for spearphishing e-mails and heightens the security of the whole ecosystem.

The fourth problem is the availability of test cases and realistic phishing mails as research corpora. If we want to have relevant, unbiased and realistic data for research, we have to collect data continuously with the help of a honeypot e-mail, and usually that will only get us low

quality mass phishing mails and no e-mails that are used in advanced or targeted attacks. And most of the time, if there are interesting cases, organizations that had breaches with targeted attacks classify the phishing e-mails as sensitive and are reluctant to share that information with third parties, which means valuable and interesting research data is hard to obtain, which means that we need to collect large data sets of phishing e-mails that would enable us to research users behavior against known samples to obtain more information about how users perceive phishing attacks and the effectiveness of such attacks.

One important measure is the gradation of the sophistication the phishing e-mails can have. On the low end of the spectrum, we have the mass attacks that try to net the most gullible of users into divulging their PayPal accounts or any other account that can be used instantly to obtain some kind of benefit for the attacker, where even slightly trained users will know how to avoid such attacks. The connection we see from real life cases shows us that the most interesting result is the point that combines the effort the attackers invested into the preparation of the attack, the elements (hooks / deception elements) they attackers used to create the phishing e-mail and finally, the information if the attackers succeeded or not. The interesting attacks are the ones that are marginally targeted, where an attacker did minimal preparation and obtained even one compromised target.

4. RESEARCH GOALS

The goal of our research was to examine the students' familiarity with threats in the form of phishing attacks conducted via the Internet. In accordance to the reasons we wrote earlier in the earlier chapter, a practical test was conducted to determine the student's ability to recognize phishing attacks and if they know how to protect themselves.

In order to present the main guidelines for protection against phishing attacks we tried to answer the following research questions:

- In what extent are students targeted by phishing attacks?
- Do awareness and habits of students help prevent phishing attacks?
- Based on which elements can we determine the students' knowledge about phishing attacks?
- Is there a statistically significant correlation between the education of students about phishing attacks and their resistance against phishing attacks?
- How well do students identify phishing attacks?
- Is there a significant difference between students in different areas of study with regard to knowledge of how to protect themselves from phishing attacks and knowing the essential characteristics of phishing attacks and social engineering?

The motivation behind this research is to explore the Croatian student population's self assessment in regard to phishing attacks and to assess their capability on a limited data set for purposes of obtaining a baseline for future research.

5. METHODOLOGY

We created an online questionnaire that contained 23 questions of which five are pictures of e-mails where the students could see all relevant data in the picture (sender, subject, addresses, URLs etc.). Four were examples of realistic, high quality phishing attacks that were conducted against test subjects' institution that were collected with the help of incident response efforts and reports by users. One sample was a legit email from a company. Participants were asked to determine if each sample is malicious, legit or if they are not sure.

First sample was an example of phishing email sent by a PayPal imitator. The main indicators of fake email were misspelled words, poor imitation of instructions, link that redirect to the fake site and link to log-in that usually PayPal does not add to content of their emails.

Second sample was a phishing email that looked like it was from IRS (Internal Revenue Service). The main indicators of fake email were that the e-mail was not addressed to the recipient and a form that demanded personal and private user data, and submit button that sent data via an unsecured connection.

Third sample was a legit email about confirmation of a recent transaction from a bank. The main indicators of legit email were the last four digits of account number, email was addressed with name of account holder and legit domain name in the URL.

Fourth sample was a phishing email sent by someone imitating “PayPal Dispute Transaction”. The main indicators of this fake email were that the e-mail was not addressed to the correct recipient, large amount of details that should convince recipient about legitimacy, and a fake URL that is similar to the legit URL, and connection via an unsecured connection.

Fifth sample was an example of a phishing email about account access. There were a few phishing indicators that are hidden and hardly noticeable. Main indicators were wrong usage of casing (uppercase/lowercase) of text in the e-mail text and one fake URL among legit content.

Based on the results of the survey we analyzed the data with the help of correlations and analysis of variance. Pearson correlation coefficient was used, which is sensitive only to the linear relationship between the variables. The correlation was performed in order to show the link between education about phishing attacks and prevention of this same attacks.

All research samples and data can be obtained in raw form by contacting the authors.

6. RESULTS

We collected 342 valid responses and determined the percentage of targeted students (students that identified that they were targeted by phishing attacks) and students who were victims of phishing attacks, where they are sure that they were successfully targeted and exploited.

Our sample consisted of students from the Faculties from seven different scientific fields of study: technical, social, humanities, natural, medical, agricultural and art sciences as shown in table 1 which were part of the University of Zagreb. The distribution of their study years is evenly distributed (see table 2).

Table 1: Distribution of students fields of study

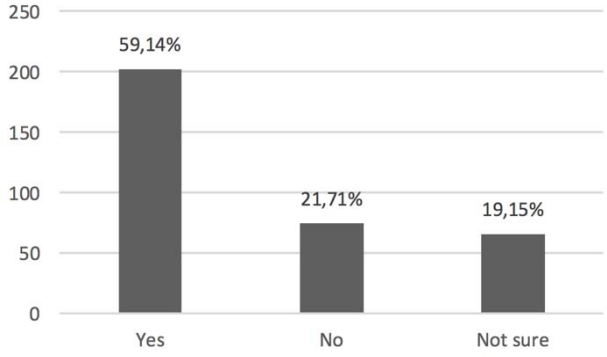
Scientific field	Students
Arts	1 (0,29%)
Technical sciences	124 (36,26%)
Natural sciences	53 (15,50%)
Agricultural sciences	23 (6,73%)
Humanistic sciences	21 (6,14%)
Medical sciences	16 (4,68%)
Social sciences	104 (30,41%)

Table 2: Distribution of students study years

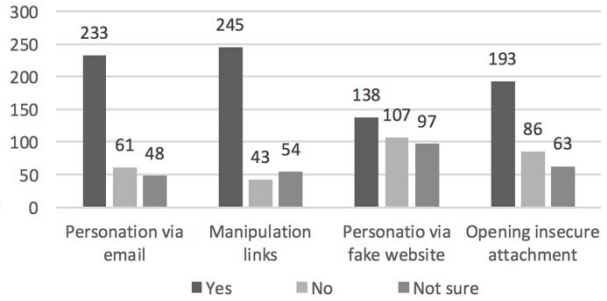
Year of study	Students
First year of study	68 (19,88%)
Second year of study	61 (17,84%)
Third year of study	69 (20,18%)
Fourth year of study	67 (19,59%)
Fifth year of study	69 (20,18%)
Postgraduate study	8 (2,34%)

Most of our test subjects, 59.14% stated that they were targets of phishing attacks while 19.5% are not sure if they were targeted so we can say that more than 59.14% students were targets of some class of phishing attack.

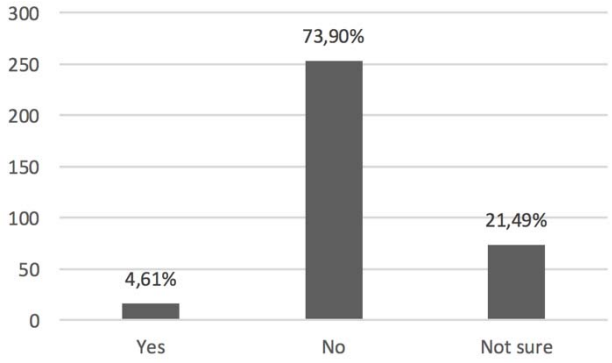
Graph 1 shows the students answers depending on their response if they were targeted, where graph 2 shows the response depending on the attack type. Graph 3 shows the overall proportion of students who were victims of phishing attacks, where students answered that 4.61% of them were victims. Most of students, 73.90% answered that they were not victims of phishing attacks while 21.49% are not sure if they were victim so we can say that more than 4.61% of students were affected by some kind of phishing attack. Graph 4 shows the proportion of students were victim of phishing attack separated by type of attack.



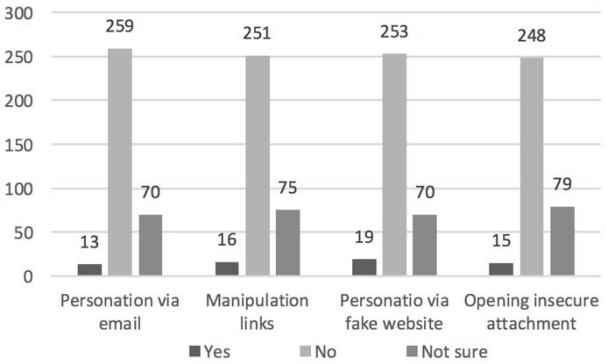
Graph 1: Proportion of students that were targeted by phishing attacks



Graph 2: Proportion of students that were targeted according to attack type



Graph 3: Proportion of students that were victims of phishing attacks



Graph 4: Proportion of students that were victims according to attack type

One interesting piece of data is the success or failure of students to identify correct phishing cases. Table 3 shows the students answers to test samples where we have underlined the wrong answers to those test cases. From table 3 and 4 we can see that the in average failure rate was 27%. The most interesting case is the fifth sample (Phish4), where we see that almost 33% of the students failed to identify the last sample as malicious, which shows that the best strategy in phishing attacks is to create a perfect clone of a legitimate web or mail and just change the core, single element with a malicious one.

Table 3: Students answers to phishing samples

Answer	Phish1	Phish2	Legit	Phish3	Phish4
Phishing attack	195 (57%)	130 (38%)	120 (35%)	127 (37%)	91 (27%)
Legit website	50 (15%)	98 (29%)	81 (24%)	78 (23%)	113 (33%)
Not sure	97 (28%)	114 (33%)	141 (41%)	137 (40%)	138 (40%)

Table 4: Students answers to phishing samples

Answer	One correct answer	Two correct answers	Three correct answers	Four correct answers	Five correct answers
%	79 (23,10%)	88 (25,73%)	65 (19,01%)	31 (9,06%)	10 (2,92%)

70% of students (7 out of 10) with all correct answers stated that they were not targeted by phishing attacks.

We also investigated relationship between self perception of knowing how to protect and number of correct answers given on five questions recognizing phishing.

Table 5: Students self assessment and capability to identify phishing attacks correlated

Answer	Number of correct answers	Number of students
Do you know how to protect yourself from phishing attacks - YES	5	9 (6,98%)
	4	21 (16,28%)
	3	35 (27,13 %)
	2	40 (31,01%)
	1	17 (13,18 %)
	0	7 (5,43 %)
Do you know how to protect yourself from phishing attacks - NO	5	1 (0,47%)
	4	10 (4,69 %)
	3	30 (14,08 %)
	2	48 (22,54 %)
	1	62 (29,11 %)
	0	62 (29,11 %)

Table 5 shows significantly higher percentage of students with no correct answers in the group of students evaluating themselves as the one that "don`t know how to protect". Furthermore, there is "higher percentage of correct answers in the group of students with self evaluation as "we know how to protect". These results demonstrate validity of students self evaluation.

We used Pearson's *r* [16], a correlation to see what variables have strong linear relationship between themselves. Correlation analysis reveals high and statistical significant correlation between students answers and the fact are they target of the attacks or not: students recognizing phishing attacks were not target of the attacks ($r = 0,68, p < 0,002$).

One field we wanted to explore is if education has any effect against phishing attacks, since it acts as a preventive measure. The following correlations between two variables and their Pearson's r value and p value indicate the importance of education in protection against phishing:

- Are you familiar with the term phishing attacks? - Do you know how to protect yourself from phishing attacks? (r = 0,5865 p = <,0001)
- Do you know the difference between http and https protocols? - Do you know how to protect yourself from phishing attacks? (r = 0,5089 p = <,0001)
- Do you know what shortened link is? - Do you know how to protect yourself from phishing attacks? (r = 0,4813 p = <,0001)

The correlation coefficient is positive if students are familiar with the concept of phishing attacks, shortened links and the difference between http and https protocols, which strongly correlates with the variable that shows that they know how to protect themselves from phishing attacks. All three correlation coefficients are between 0,4 and 0,7 which indicates that they are significant. These correlations provide confirmation to the fourth research question: Is there a statistically significant correlation between the education of students about phishing attacks and protect against phishing attacks?

The following correlations indicate importance of awareness and habits that prevents user from becoming a victim of phishing attack:

- Are you familiar with the term phishing attacks? - Do you know how to protect yourself from phishing attacks? (r = 0,5865 p = <,0001)
- Do you know what are shortened links? - How often do you check the URL after the opening new website link? (r = 0,4142 p = <,0001)
- Do you know how to protect yourself from phishing attacks? - How often do you check the URL after the opening new website link? (r = 0,4419, p = <,0001)

Other interesting correlations are shown in table 6. If student has a habit to check URL after opening the website link, he is more likely not to become a victim of phishing attacks. Also, not knowing about URL shorteners and not having habits like checking URLs after opening new website link, leads to students' vulnerability and students are more exposed to attacks. With these correlations we confirm research question: Do awareness and habits of students helps prevent phishing attacks?

Table 6: Interesting correlations

Variable X	Variable Y	r	p - value
Do you know how to protect yourself from phishing attacks?	Are you familiar with the term phishing attacks?	0,5865	<,0001
Are you familiar with the term social engineering?	Are you familiar with the term phishing attacks?	0,5233	<,0001
Do you know the difference between http and https protocols?	Do you know how to protect yourself from phishing attacks?	0,5089	<,0001
Do you know what the shortened links are?	Do you know how to protect yourself from phishing attacks?	0,4813	<,0001
Do you know what the shortened links are?	Are you familiar with the term phishing attacks?	0,4588	<,0001
Do you know the difference between http and https protocols?	Do you know what the shortened links are?	0,4450	<,0001
Do you know the difference between http and https protocols?	Are you familiar with the term phishing attacks?	0,4392	<,0001
Do you know what the shortened links are?	How often do you check the URL after the opening new website link?	-0,4142	<,0001
Do you know how to protect yourself from phishing attacks?	How often do you check the URL after the opening new website link?	-0,4419	<,0001

Analysis of variance [16] was used to indicate whether there is a difference between the students' areas of study and Faculty in understanding the characteristics of phishing attacks. We saw that variability inside groups is bigger than variability between groups and that indicates difference in understanding the characteristics which is shown in table 7. The results of the ANOVA include Sum of Squares, df (degrees of freedom), Mean Square, F (for F-ratio). Critical for interpretation is statistical significance of the results. Thus, table 7 highlights only statistical significant differences.

The question "Do you know how to protect yourself from phishing attacks?" showed promising variable quality between and inside groups.

Between groups:

- SumOfSquares = 11.167,
- df = 6,
- MeanSquare = 1.861
- F = 9.013 and p = 0.000.

Inside groups:

- SumOfSquares = 69.175
- df = 335
- MeanSquare = 0.206
- F = 9.013
- p = 0.000

Table 7: ANOVA for interesting variables (p=0.000)

		Sum of Squares	df	Mean Square	F
Are you familiar with the term phishing attacks?	Between/ Within Groups	27.759/ 168.081	6/ 335	4.626/ 0.502	9.221
How often do you check the URL after the opening new website link?	Between/ Within Groups	49.055/ 597.498	6 /335	8.176/ 1.784	4.584
Do you know how to protect yourself from phishing attacks?	Between/ Within Groups	11.167/ 69.175	6 /335	1.861/ 0.206	9.013
Do you know the difference between http and https protocols?	Between/ Within Groups	26.422/ 56.084	6 /335	4.404/ 0.167	26.304
Are you familiar with the term social engineering?	Between/ Within Groups	10.393/ 117.770	6 /335	1.732/ 0.352	4.927

Table 7 indicates highest differences between students in different scientific fields in the URL checking after the opening new link. Furthermore, the lowest difference within the students in the same scientific fields is in the knowing of the difference between http and https protocols. With this results we can say that there is a statistically significant difference between students in different areas of study, where as expected, computer science and informatics students had the best resistance against phishing attacks. Such trends show the need for information security awareness education for students that study in other areas of study.

7. FUTURE GOALS

Research into phishing and social engineering is a very interesting area since a significant number of attacks are conducted with the help of social engineering and phishing as the main vector to either obtain credentials or trick the user into executing a malware infected file. Our research wasn't designed to deliver significant state of the art results, but it was designed to explore the area of research for

potential future studies. Such a limited pilot study showed interesting challenges with this area of research, mostly because high quality phishing samples that are used against real users is hard to obtain, and 'invented' research data is still biased by the researcher. We see two possible improvements in this field if we collect a significant amount of valid, realistic phishing and spearphishing e-mails for a research corpus. First would be the possibility to identify interesting patterns in phishing e-mails that would help us to train users to detect deception or to develop new methods that would rely on machine learning and pattern recognition to filter out and tag possible phishing mails in a way that would not rely on definitions like antivirus programs.

8. CONCLUSION

Our analysis showed disturbing results: more than 59% of students were targeted by phishing attacks. The answered research questions indicate the crucial need for additional education and guidelines for prevention of phishing attacks for students in Croatia. With given correlations we can see that students without theoretical knowledge about phishing attacks are gullible and susceptible to phishing attacks. Some of the interesting results our research are:

- 21,71% of the students' state that they haven't been targets of phishing attacks, 19.5% of the students' state that they are not sure
- In average 25% of the students failed to correctly identify phishing attacks
- 4,61% of the students say they were a victim of phishing attacks, 21% are not sure.
- The most effective attack was a page that was a perfect clone of a regular, valid mail with only the main action URL rerouting to a phishing domain.
- The single most relevant fact that helped users correctly identify phishing attacks was the familiarity with phishing attacks and if they were educated about those classes of attacks and if they are aware if the correct URL or protocol is used for communication.

REFERENCES:

[1] Stavroulakis, Peter, and Mark Stamp, eds. Handbook of information and communication security. Springer Science & Business Media, 2010.

[2]. Nohlberg, Marcus: Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks, Stockholm 2008. Accessed: 16.02.2016. Online:http://www.diva-portal.org/smash/get/diva2:200190/FULLTEXT01.pdf

[3]. The Most Popular Social Engineering Lures Used in 2014, Trend Micro, 2015. Accessed: 16.02.2016. Online: http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-most-popular-social-engineering-lures-used-in-2014

[4]. Croatian National Cert: Phishing napadi CCERT-PUBDOC-2005-01-106, Carnet, 2005. Accessed: 16.02.2016. Online: http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-01-106.pdf

[5]. The State of Security: 5 Social Engineering Attacks to Watch Out For, David Bisson, Tripwire, 2015. Accessed: 16.02.2016. Online: ttp://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

[6] Higgins, Stan: Details of $5 Million Bitstamp Hack Revealed; Online: http://www.coindesk.com/unconfirmed-report-5-million-bitstamp-bitcoin-exchange/ (Available on 18.2.2016)

[7] Mohebzada, J. G., El Zarka, A., BHojani, A. H., Darwish, A. (2012, March). Phishing in a university community: Two large scale phishing experiments. InInnovations in Information Technology (IIT), 2012 International Conference on (pp. 249-254). IEEE.

[8] Sheng S, Holbrook M, Kumaraguru P, Cranor LF, Downs J. Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. InProceedings of the SIGCHI Conference on Human Factors in Computing Systems 2010 Apr 10 (pp. 373-382). ACM.

[9] Dodge RC, Carver C, Ferguson AJ. Phishing for user security awareness. Computers & Security. 2007 Feb 28;26(1):73-80.

[10] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

[11] Sheng S, Magnien B, Kumaraguru P, Acquisti A, Cranor LF, Hong J, Nunge E. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. InProceedings of the 3rd symposium on Usable privacy and security 2007 Jul 18 (pp. 88-99). ACM.

[12] Wang J, Herath T, Chen R, Vishwanath A, Rao HR. Research Article Phishing Susceptibility: An Investigation Into the Processing of a Targeted Spear Phishing Email. Professional Communication, IEEE Transactions on. 2012 Dec;55(4):345-62.

[13] Abdelhamid N. Multi-label rules for phishing classification. Applied Computing and Informatics. 2015 Jan 31;11(1):29-46.

[14] Lakshmi VS, Vijaya MS. Efficient prediction of phishing websites using supervised learning algorithms. Procedia Engineering. 2012 Dec 31;30:798-805.

[15] Rao RS, Ali ST. PhishShield: A Desktop Application to Detect Phishing Webpages through Heuristic Approach. Procedia Computer Science. 2015 Dec 31;54:147-56.

[16] Field, Andy P, Jeremy Miles, and Zoë Field. Discovering Statistics Using R. London: Sage, 2012. Print.