УДК 004.6:004.738.5
DOI: https://doi.org/10.22182/spm.6312019.10
Прегледни рад

Српска политичка мисао
број 1/2019.
год. 26. vol. 63
стр. 189-207

Синиша Домазет*

Факултет за студије безбедности, Универзитет Едуконс, Сремска Каменица

Здравко Скакавац

Факултет за правне и пословне студије др Лазар Вркатић, Нови Сад, Универзитет Унион, Београд

„ФИШИНГ“ – ИЗАЗОВ У ЗАШТИТИ БЕЗБЕДНОСТИ ПОДАТАКА КОРИСНИКА ИНТЕРНЕТА**

Сажетак

Циљ истраживања у раду је анализа једног од облика високотехнолошког криминала, који носи назив фишинг („пецање“). Истраживањем је утврђено да је број фишинг превара широм света у порасту из године у годину, са великим штетама. Облици и начини извршења овог вида преваре еволуирали су током времена и постали све софистицираније и самим тим, тежи за откривање. Показало се да су фишинг нападима погођени не само грађани, већ и привредни субјекти и важне државне институције. У раду су приказани примери фишинг напада у свету и у Републици Србији. Анализа је показала да је Република Србија све више угрожена услед фишинг напада и да не постоји *lex specialis* којим је уређено ово питање. Утврђено је да је неопходно предузети бројне превентивне мере за спречавање крађе приватних података и других значајних информација. То подразумева повећан опрез код отварања мејлова, пажљиво читање њиховог садржаја, избегавање „клика“ на сумњиве линкове чиме се активирају малициозни софтвери, повећан опрез код електронске

* Електронска адреса аутора: sdomazetns@gmail.com.

** Овај рад је део истраживачког пројекта под шифром 47009 (Европске интеграције и друштвено-економске промене привреде Србије на путу ка ЕУ), финансираног од стране Министарства просвете, науке и технолошког развоја Републике Србије.

трговине и коришћења кредитних картица и друге мере. У раду је указано на потребу доношења посебног закона који би уредио област фишинг преваре, као и пооштравање казнене политике. У раду су коришћени нормативни метод и правно-логички методи индукције и дедукције.

Кључне речи: право, Европска унија, безбедност, фишинг, интернет

1. ПОЈАМ И ОБЛИЦИ „ФИШИНГА“

У ери убрзаног развоја информационо-комуникационих технологија све су присутнији различити облици злоупотреба у погледу коришћења интернета. Оне се огледају у нарушавању поверљивости информација, ометању њихове функционалности кроз поремећаје операција међу њима, узурпирању и крађи интелектуалних добара, разним врстама других крађа и превара, као и многобројним злоупотребама које се разликују по мотивима, циљевима, методима и начинима остваривања.[1] Појам крађе повезане са информационо-комуникационим технологијама, поред крађе која се изводи тако да се отуђују информационо-комуникациони уређаји и њихове компоненте, подразумева крађу разноврсне робе, крађу рачунарских услуга, крађу података, крађу кодова, лозинки и идентификационих бројева и крађу идентитета.[2]

У том смислу, „фишинг“ и крађа идентитета све више постају доминантан облик активности извршилаца кривичних дела у области високотехнолошког криминала. Из дана у дан све су уочљивије модификације ових феномена, а инвентивност криминалаца је у складу са информационим окружењем-нови трендови су такви да је веома тешко пратити их у реалном времену. Широм света уочава се талас професионализације извршилаца кривичних дела за ове технике које су им од великог, и у многим кривичним делима од кључног значаја у почетним стадијумима вршења кривичног дела[3].

Термин „фишинг“ (*phishing*, пецање) се први пут појавио 1996. године када је група хакера украла корисничка имена и лозинке рачуна AOL путем поруке електронске поште, „удице“ на коју су се корисници сервиса AOL „упецали“.[4] Сам термин потиче из

1) Анђелија Ђукић, „Крађа идентитета-облици, карактеристике и распрострањеност”, *Војно дело*, Министарство одбране, бр. 03/2017, стр. 99.

2) Слободан Петровић, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004, стр. 133.

3) Владимир Урошевић, Звонимир Ивановић, Сергеј Уљанов, *Мач у world wide web-у (изазови високотехнолошког криминала)*, Eternal mix, Београд, 2012, стр. 175.

4) Исто.

аналогије да преваранти користе електронску пошту као мамац за рибу за профитабилне личне податке из неподозривог мора корисника интернета.[5] Фишинг се односи на метод коришћен од стране крадљиваца идентитета ради прибављања личних података (као што су имена, шифре, бројеви социјалног осигурања[6], подаци о кредитним картицама), коришћењем злонамерних *e-mail* порука које изгледају као да потичу из легитимног пословања.[7]

Приликом извођења фишинг напада користи се комбинација техничке преваре и такозваног социјалног инжењеринга. У већини случајева, вршилац преваре мора да убеди своју жртву да намерно изведе серију активности које ће обезбедити приступ поверљивим информацијама. За извођење фишинг напада најчешће се користе комуникациони канали као што су електронска пошта, веб-странице, различите апликације као што је IRC, или сервиси за слање порука. У сваком случају, преварант мора изгледати као поверљив извор (као што је сервис за помоћ банака, аутоматизована подршка од омиљеног онлајн препродавца, и слично), како би жртва преваре поверовала.[8]

У почетним етапама развоја фишинга извршиоци су се користили релативно једноставним методама преваре, тако да су фишинг мејлови били релативно лако препознатљиви (примера ради, садржали су бројне граматичке и словне грешке), док је данас фишинг еволуирао и постао много комплекснији и софистицираније, укључујући коришћење бројних напредних софтверских решења за прикривање како би се прибавили осетљиви (лични) подаци.

Класични фишинг напад се одвија по следећем обрасцу. У првој фази, преварант (енг. "*Phisher*") шаље *e-mail* који изгледа као да потиче из легитимног пословања. Ово се најчешће постиже коришћењем блиских робних марки, трговачких имена или других општих корпорацијских идентификатора. Потом, у другој фази, интернет провајдер испоручује *e-mail* до интернет корисника. Притом, тај мејл обично ствара лажан осећај хитности, информисањем корисника да постоји проблем са његовим/њеним налогом. Након тога, мејлом се траже лични подаци од корисника у циљу валидирања налога. У трећој фази, прималац мејла „укуцава"

5) Scot Graydon, "Phishing and Pharming: The New Evolution of Identity Theft", *Consumer Financial Law quarterly Report*, бр. 60/2006, стр. 335, 337.

6) Ово је нарочито важан податак у САД.

7) Scot Graydon, "Phishing and Pharming: The New Evolution of Identity Theft", нав. дело, стр. 335-336.

8) Gunter Ollmann, *The Phishing Guide (Understanding & Preventing Phishing Attacks)*, NGS-Software Insight Security Research, United Kingdom, 2004, Internet: https://www.nccgroup.trust/uk/our-research/the-phishing-guide-understanding-preventing-phishing-attacks/, 14/07/2018.

личне податке или „кликне“ на лажни веб-сајт који имитира изглед организације/компаније поменуте у мејлу. Најзад, у четвртој фази, преварант користи тако добијене информације како би починио крађу идентитета и касније га злоупотребио[9].

Електронске поруке које се користе у овој превари обично имају облик лажних упозорења банака или других финансијских организација да ће доћи до гашења рачуна клијента ако не унесе или ако не ажурира одређене податке, лажних порука администратора у којима се траже кориснички подаци као што је лозинка, поруке у којима се позива на безбедност и од корисника захтева да открију личне податке (кориснички рачун, лозинку), или се захтева инсталација неког програма ради отклањања откривеног безбедносног пропуста, порука у којима се корисник обавештава да је добио на лутрији, због чега треба да достави одређене податке да би могао подићи добитак, и слично.[10]

Постоји неколико *облика фишинга*.

Први од њих представља такозвани „циљани фишинг“ (енг. *Spear phishing*). У односу на раније облике, циљани фишинг је усмерен према тачно одређеним лицима, пре свега високорангираним службеницима у компанијама, државним институцијама, владиним агенцијама и томе слично. Дакле, реч је о фишингу који се односи на тачно одређени круг индивидуалаца. С обзиром да мејлови који се шаљу од стране преваранта изгледају аутентично (поруке могу изгледати као да долазе од руководиоца или надређеног), већа је вероватноћа да дође до откривања важних података којима ова лица располажу, те и штете могу бити много озбиљније.

Други облик фишинга који се појавио у пракси се назива „фарминг“ (енг. *Pharming*).[11] Овде је, заправо, реч о савременијој форми фишинга, где се користе злонамерни софтвери (вируси), као што су такозвани „тројанци“, којима се модификује фајл хоста или DNS (енг. *Domain Name System*). На тај начин, долази до преусмеравања корисника са интернет сајта који је желео да посети на лажни интернет сајт, а да притом он тога није ни свестан. На тај начин, корисник (верујући да се налази на жељеном сату, на пример сајту своје банке) уноси своје личне податке у базу података лажног вебсајта и тако омогућава преваранту да дође до осетљивих

9) Rasha Almahroos, “Phishing for the Answer: Recent Developments in Combating Phishing”, *A Journal of Law and Policy for the Information Society*, Ohio State University, Moritz College of Law, United States, бр. 3/2007, стр. 596-597.

10) Владимир Урошевић, Звонимир Ивановић, Сергеј Уљанов, *Мач у world wide web-у (изазови високотехнолошког криминала)*, нав. дело, стр. 177.

11) За овај облик фишинга се у литератури користи и назив “*Domain Spoofing*”.

информација о кориснику. Иако је фарминг један од облика фишинга, разлика је у томе што се код фишинга жртве нападају једна по једна, а код фарминга се у кратком временском интервалу напада огроман број корисника интернета који се без своје воље или воље институције чији је интернет сајт нападнут преусмеравају на лажни интернет сајт и остављају осетљиве податке[12].

Трећи облик фишинга се назива „вишинг" (енг. *Vishing*)[13]. За разлику од класичног фишинга и фарминга, код вишинга се превара врши уз помоћ телефона и интернета. Наиме, преварант шаље жртви лажан мејл који изгледа као мејл неке банке или неког познатог сервиса за електронску куповину (на пример, *eBay*). У мејлу се обично наводи да је рачун жртве (клијента) угашен/онемогућен и да се мора контактирати банка (извор) како би се „проблем" са рачуном решио. У мејлу преваранти оставе број телефона који жртва може да позове, како би оставила личне податке и друге информације. Разуме се, на овај начин преваранти лако долазе до осетљивих података, које касније продају или злоупотребљавају на многобројне начине.

Без обзира о ком облику фишинга је реч, много тога зависи од свести корисника интернета о „пецању", посебно узимајући у обзир све софистицираније форме фишинга. Поменуто је раније да је фишинг у почетку подразумевао слање мејлова који су били релативно лако препознатљиви као злонамерни (услед бројних словних, граматичких и других грешака). Међутим, у модерно време се користе све опаснији злонамерни софтвери (вируси) како би се од жртава изнудили осетљиви лични подаци (шифре, подаци о платним картицама, али и други подаци које корисник откуца на тастатури). Међу злонамерним софтверима за крађу личних података истичу се *Trojan keylogger*, *mouse loggers*, као и *screen grabers*, уз помоћ којих се прибављају подаци о куцању карактера на тастатури зараженог рачунара, активностима миша, односно активностима на монитору заарженог рачунара. Банке су на више начина покушавале да „доскоче" преварантима, креирајући различите механизме за одбрану од фишинга, али пракса је показала да криминалци прибегавају све напреднијим методама за крађу података од корисника банкарских услуга. Стога, може се закључити да борба између банака и компанија са једне стране и превараната са друге стране траје несмањеним интензитетом.

12) Владимир Урошевић, Звонимир Ивановић, Сергеј Уљанов, *Мач у world wide web-у (изазови високотехнолошког криминала)*, нав. дело, стр. 191-192.

13) У литератури се користи и назив "*Voice Phishing*".

2. ПРИМЕРИ ФИШИНГА

Пракса показује да је распрострањеност фишинга велика и да је погођен практично цео свет. Само током 2015. године у свету је регистровано око 147 милиона фишинг напада, од тога највише напада је претрпела Русија (17,8%), док су САД биле најбољи „домаћин" нападачима и са њене територије је извршено највише напада (15,2%). Према циљу, фишинг напади су највише били усмерени на онлајн финансијске институције (банке, системи плаћања и онлајн продавнице)[14]. У 2016. години регистровано је преко 154 милиона фишинг напада, при чему је Бразил претрпео највише напада, а преко 12% напада је потицало из САД. У 2017. години забележено је преко 246 милиона напада, а највећи извор напада и у овој години остале су САД (са уделом од 13,21%). Највише је коришћен малвер под називом *Trojan-Downloader.JS.Sload.*[15] Може се закључити да број фишинг напада расте из године у годину, док су злонамерни софтвери све опаснији. Посебно забрињава чињеница да се наведени подаци односе на случајеве у којима су се активирали антифишинг системи, тако да се лако долази до закључка да је фишинг напада у стварности било далеко више. Европска унија је такође изразила велику забринутост због повећаног броја фишинг напада, посебно у 2017. години,[16] што се може илустровати са више различитих примера широм света.

На пример, почетком 2017. године извршен је циљани фишинг у виду лажних мејлова, који су изгледали као да су послати од стране директора компанија, а у њима је тражено од запослених да доставе личне податке у вези са порезом (такозвани *W-2 Phishing scam*). На овај начин је компромитовано више од 120 хиљада запослених у више од 100 различитих организација.[17]

У мају 2017. године дошло је до напада уз помоћ малициозног софтвера, такозваног „црва" *WannaCry*, који је користио слабости у оперативним системима Мајкрософта, како би „инфицирао"

14) Анђелија Ђукић, „*Крађа идентитета-облици, карактеристике и распрострањеност*", нав. дело, стр. 110.

15) Darya Gudkova, Maria Vergelis, Tatyana Shcherbakova, Nadezhda Demidova, *Spam and phishing in 2017 on February 15, 2018. 10:00 am*, *Securelist. 15.02.2018,* Internet, https://securelist.com/spam-and-phishing-in-2017/83833, 15/07/2018.

16) European Union Agency for Network and Information Security (ENISA). *ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends*, стр. 42, Internet, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, 17/07/2018.

17) Small Business Trends *W-2 Phishing Scam Threatening Small Business After Tax Day*, 02.05.2017, Internet, https://smallbiztrends.com/2017/05/w-2-phishing-scam-small-business.html, 16/07/2018

рачунаре. Када би рачунар био заражен, долазило је до енкрипције оперативног система и чинило их неупотребљивим. Након тога, хакери су тражили од жртава одређену надокнаду како би откључали криптовани софтвер.[18] Истог месеца, око 3 милиона радника широм света су били жртве хакерског напада у виду злонамерних мејлова који су садржали позиве на *Google docs* и позивали примаоце да „едитују" документе. Чим су позиви отворени, примаоци су преусмерени на апликације трећих лица које су омогућиле хакерима приступ *Gmail*-налозима жртава[19].

У јуну 2017. године хакери су уз помоћ рансомвер-а (енг. *Ransomware*) напали компаније, спречавајући их да приступе подацима док жртве не уплате откуп у износу од 300 америчких долара, овог пута не у новцу, већ у битокин криптовалути (*Petya Cyber Attack*). Једна од жртава била је и позната компанија Маерск (*Maersk*)[20]. Потом, у јулу 2017. године, компанија из области безбедности на интернету под именом *Comodo* открила је нови облик фишинг преваре, усмерене превасходно на мала предузећа. Тада је фишинг мејл послат на *e-mail* адресе преко 3.000 привредника, под називом „достава информација". У мејлу се налазило обавештење о предстојећој испоруци од стране *United Parcel Service* (UPS) и укључивало је и наизглед безазлен линк (који је садржао малвер). У случају када би прималац мејла „кликнуо" на линк ризиковао је ослобађање опасног вируса, који би фишинг-преварантима омогућио прибављање података[21].

Исте године је извршен сличан напад на више од 500 индустријских компанија, а у фишинг превари се у мејловима (који су садржали малвер) од прималаца тражило да „скину" малициозни фајл. Чим су жртве то урадиле, преварантима је био омогућен приступ пословним подацима и мрежи (*Business Email Compromise*-BEC).[22] Такође, у 2017. години и пословни свет у држави Катар је био мета

18) Pysis.net, *WannaCry Exposes Extent of Cyber Crime Threat to Small Business*, 12.06.2017, Internet, https://www.pisys.net/blog/wannacry-exposes-extent-of-cyber-crime-threat-to-small-business.asp, 16/07/2018.

19) BBC, *Google Docs users hit by phishing scam*, 04.05.2017, Internet, https://www.bbc.co.uk/news/business-39798022, 16/07/2018.

20) The Guardian, *'Petya' ransomware attack: what is it and how can it be stopped?*, 28.06.2017, Internet, https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how, 16/07/2018.

21) BBB News, *Newly Identified Phishing Attack Targeting Small Businesses*, 20.07.2018, Internet, https://www.bbbwminews.org/single-post/2017/07/20/Newly-Identified-Phishing-Attack-Targeting-Small Businesses, 16/07/2018.

22) SC Media, *Nigeria-based BEC scams pulling in millions, SecureWorks report*, 05.08.2016, Internet, https://www.scmagazine.com/nigeria-based-bec-scams-pulling-in-millions-secureworks-report/article/528085/, 16/07/2018.

хакерског напада (више десетина хиљада фишинг напада за три месеца). Напад се такође састојао у слању злонамерних мејлова и смс-порука пословним људима, у циљу стицања осетљивих личних података и информација. Притом, само у првом кварталу 2017. године у Катару је забележено преко 90 хиљада фишинг напада[23]. Треба споменути и познати случај *Amazon Prime Day phishing attack*, када су хакери слали злонамерне мејлове корисницима Амазона. У мејловима су се налазиле наизглед легитимне понуде клијентима Амазона. Чим би клијенти покушали да купе понуђено, трансакције се не би обавиле, а онда се тражило од жртава да унесу податке који би могли бити компромитовани и украдени.[24]

Чак је и на последњем првенству света у фудбалу, у Русији, 2018. године, забележен велики број сајбер напада. Поменути сајбер напади су били у директној вези са светским првенством, а регистровано је готово 25 милиона сајбер напада.[25] Иако експлицитно није поменуто, сасвим сигурно се велики проценат ових напада односи на фишинг.

3. ПРАВНА РЕГУЛАТИВА ЕУ И РЕПУБЛИКЕ СРБИЈЕ У ОБЛАСТИ ФИШИНГА

Узимајући у обзир велику опасност од сајбер напада, а посебно од фишинга, Европска унија је реаговала и на легислативном плану. Притом, не постоји посебан акт који се односи искључиво на фишинг, већ је фишинг непосредно или посредно обухваћен неколицином аката, од којих треба истаћи следеће акте: Оквирна одлука Савета о борби против превара и кривотворења безготовинских средстава плаћања, Директива 2016/1148 Европског парламента и Савета о мерама за висок заједнички ниво безбедности мрежних и информационих система широм Уније, Директива 2013/40/ЕУ Европског парламента и Савета о нападима на информационе системе и о замени Оквирне Одлуке Савета 2005/222/PUP, Уредба (ЕУ) бр. 526/2013 Европског парламента и Савета о Агенцији Европске уније за мрежну и информациону безбедност (ENISA) и о стављању ван снаге Уредбе (ЕЗ) бр. 460/2004, Конвенција

23) Gulf Times, *Qatar faced 93,570 phishing attacks in first quarter of 2017*, 12.03.2017, Internet, http://www.gulf-times.com/story/547784/Qatar-faced-93-570-phishing-attacks-in-first-quart, 16/07/2018.

24) Kimkomando, *Amazon Prime Day phishing scam spreading now!*, 21.08.2017, Internet, https://www.komando.com/happening-now/415020/amazon-prime-day-phishing-scam-spreading-now, 16/07/2018.

25) TVN1, *Tokom Mundijala sprečeno 25 miliona sajber napada*, Internet, http://rs.n1info.com/a404278/Svet/Svet/Tokom-Mundijala-spreceno-25-miliona-sajber-napada.html, 16/07/2018.

Савета Европе о високотехнолошком криминалу, Директива 2009/136/ЕЗ Европског парламента и Савета од 25. децембра 2009. о измени Директиве 2002/22/ЕЗ о универзалним услугама и правима корисника с обзиром на електронске комуникационе мреже и услуге (Директива о универзалним услугама), Директиве 2002/58/ЕЗ о обради личних података и заштити приватности у сектору електронских комуникација (Директива о приватности и електронским комуникацијама) и Уредбе (ЕЗ) бр. 2006/2004 о сарадњи између националних тела одговорних за спровођење закона о заштити потрошача, Комуникација из 2006. године од стране Европске комисије Европском парламенту, Савету, Европском економском и социјалном комитету и Комитету Региона о борби против спама, спајвера и злонамерних софтвера, Директива 2005/29/ЕЗ Европског парламента и Савета о непоштеној пословној пракси пословног субјекта у односу према потрошачу на унутрашњем тржишту и о измени Директиве Савета 84/450/ЕЕЗ, директива 97/7/ЕЗ, 98/27/ЕЗ и 2002/65/ЕЗ Европског парламента и Савета, као и Уредбе (ЕЗ) бр. 2006/2004 Европског парламента и Савета (такозвана Директива о непоштеној пословној пракси), Директива 2002/58/ЕЗ о обради личних података и заштити приватности у сектору електронских комуникација (Директива о приватности и електронским комуникацијама, такозвана *E-Privacy Directive*).

Посебно је значајна најновија Уредба (ЕУ) 2016/679 Европског парламента и Савета о заштити појединаца у вези са обрадом личних података и о слободном кретању таквих података, те стављању ван снаге Директиве 95/46/ЕЗ (Општа уредба о заштити података)[26], која се примењује на обраду личних података која се у целини обавља аутоматизовано, као и на неаутоматизовану обраду личних података који чине део система похране или су намењени да буду део тог система[27].

За фишинг је релевантно неколико чланова ове Уредбе.

Пре свега, у члану 7. Уредбе, наводи се да, у случају када се обрада података заснива на дозволи, водитељ обраде мора бити у стању да докаже да је испитаник дао дозволу за обраду својих личних података. Уколико испитаник да дозволу у виду писане

26) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 04.05.2016, стр. 1–88.

27) Синиша Домазет, Здравко Скакавац, „Скандал „Кембриџ Аналитика"-нови изазов у заштити података о личности?", *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 2/2018., стр. 120.

изјаве која се односи и на друга питања, захтев за дозволу мора бити предочен на начин да се може јасно разликовати од других питања, у разумљивом и лако доступном облику, уз употребу јасног и једноставног језика. Сваки део такве изјаве који представља кршење ове Уредбе није обавезујући. Испитаник има право у сваком тренутку повући дозволу, али повлачење дозволе не утиче на законитост обраде на основу дозволе пре њеног повлачења. Кад се процењује да ли је дозвола била добровољна, у највећој могућој мери узима се у обзир да ли је, између осталог, извршење уговора, укључујући пружање услуге, условљено дозволом за обраду личних података која није неопходна за извршење тог уговора. Дакле, водитељ обраде мора бити у стању да докаже да је испитаник дао дозволу за обраду својих личних података.

Даље, у члановима 25. и 32. Уредбе се указује на потребу за применом ефикасне заштите (техничке и организационе мере) која омогућава способност обезбеђења трајне поверљивости, целовитости, доступности и отпорности система и услуга обраде, односно система заштите који може блокирати, детектовати или отклонити негативне ефекте малвера. Такође, од компанија које прикупљају и обрађују личне податке од грађана ЕУ тражи се да примене свеобухватне мере безбедности података, као што су псеудонимизација, за омогућавање ефикасне примене начела заштите података, као што је смањење количине података, али и укључење заштитних мера у обраду како би се испунили захтеви из Уредбе. Даље, у члановима 33. и 34. Уредбе истиче се да су организације које обрађују податке у обавези да, у случају повреде личних података, без одлагања о томе обавесте надлежно надзорно тело о датој повреди, осим ако није вероватно да ће повреда личних података проузроковати ризик за права и слободе појединца. Такође, у члану 33. Уредбе се наводи да водитељ обраде података мора да поседује капацитете за решавање, односно ублажавање последица повреде података. У том погледу, водитељ обраде ће документовати све повреде личних података, укључујући чињенице у вези са повредом личних података, њене последице, као и мере предузете за отклањање штете.

Без обзира на решења Уредбе, у пракси је регистрован све већи број фишинг превара које се односе на ову уредбу, чак и пре њеног ступања на снагу. Тако, компанија из области безбедности *Redscan*, која ради ван Велике Британије, известила је о првој фишинг превари која се односи на Уредбу, а у овој превари хакери су се представили као тим за подршку клијентима компаније *Airbnb*-а. Наиме, компанија *Airbnb* је обавестила своје кориснике да ће

промене у њеној пословној политици наступити на дан ступања на снагу Уредбе, 25. маја 2018. године. Хакери су ту информацију искористили и жртвама послали сличан мејл у коме се тражило да клијенти унапреде њихове информације о налозима, тако што би „кликнули" на линк у мејлу. Наравно, радило се о мејлу који је садржао малвер уз помоћ којег су фишинг преваранти покушали да украду личне податке. Мејл је садржао и лого те компаније, цитирајући чак и Уредбу као разлог да се „кликне" на остављени (лажан) линк. Компанија *Airbnb* је упутила саопштење у којем је упозорила на опасност од злонамерног мејла и оставила могућност да јој жртве преваре пријаве превару на остављени мејл.[28]

Сличан проблем настао је и након ступања на снагу Уредбе, а односио се на компанију *Apple*. У пракси су хакери слали велики број лажних мејлова корисницима мобилних телефона и других уређаја ове компаније, у којима су обавештавали жртве како им је наводно њихов *Apple ID* закључан и биће обрисан у року од три дана уколико не испуне образац са личним подацима како би „потврдили" информације о налогу.[29] Разумљиво, и овде се радило о злонамерном фишинг мејлу, у циљу крађе и злоупотребе личних података.

Кад је реч о Републици Србији, такође не постоји *lex specialis* који се односи на фишинг, већ је овај вид високотехнолошког криминала обухваћен неколицином постојећих прописа, као што су Закон о електронској трговини[30] и Кривични законик Републике Србије (у даљем тексту: КЗРС).[31] Треба истаћи да највеће базе података о грађанима поседују Министарство унутрашњих послова (евиденција о личним картама), Републички фонд за здравствено осигурање (подаци из здравствених картона, фактуре о издатим лековима и лекарским интервенцијама), Фонд пензијског и инвалидског осигурања (евиденција пензионих осигурања), велике банке (поред исцрпне базе података о својим клијентима, имају и посебно осетљиве здравствене податке које прикупљају приликом одлучивања о кредитним захтевима) и велика је опасност за злоупотребу ових података и повреду приватности уколико се они открију.[32]

28) Infosecurity, *Airbnb Customers Targeted with Phishing Scam*, 04.05.2018, Internet, https://www.infosecurity-magazine.com/news/airbnb-customers-targeted-with/, 18/07/2018.

29) KasperskyLab, *GDPR bustle: Even scammers have new privacy policies*, 29.05.2018., Internet, https://www.kaspersky.com/blog/apple-gdpr-phishing/22517/, 18/07/2018

30) Закон о електронској трговини, *Сл. гласник Републике Србије*, бр. 41/2009 и 95/2013.

31) Кривични законик Републике Србије, *Сл. гласник Републике Србије*, бр. 85/2005, 88/2005 –испр. 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016).

32) Вида Вилић, *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета* (докторска дисертација), Ниш, 2016., стр.116.

Највећи ризик за крађу идентитета постоји уколико се сазна јединствени матични број грађана, јер на основу њега може да се „уђе“ у базу података. Процењује се да у Србији постоји велики број људи којима на адресу стижу рачуни за разна дуговања или пријаве за утају пореза у вези са пословањем предузећа чији су „власници“ иако за њих први пут чују. На туђе име се отварају фирме, подижу кредити, купује роба и сл.[33]

Кад је реч о фишингу, примењује се неколико чланова Кривичног законика Републике Србије: члан 208. (превара), члан 238. (неовлашћена употреба туђег пословног имена и друге посебне ознаке робе или услуга), члан 243. став 4. (фалсификовање и злоупотреба платних картица), члан 301. (рачунарска превара).

У Закону о електронској трговини важно је истаћи члан 8. у коме се наводи да је коришћење електронске поште у сврху слања нетражене комерцијалне поруке, дозвољено само уз претходни пристанак лица коме је таква врста поруке намењена, у складу са законом. Новчаном казном од 100.000 до 1.500.000 динара казниће се за прекршај правно лице - пружалац услуга, ако пошаље нетражену комерцијалну поруку без претходног пристанка лица којем је таква порука намењена.

Кад је реч о *примерима фишинг превара у Републици Србији*, једна од најозбиљнијих фишинг превара десила се 2017. године, а у вези са Народном банком Србије. Превара је извршена на тај начин што је путем модификоване електронске адресе 26. априла 2017. године Народна банка Србије добила нове инструкције за плаћање. Наиме, уместо са адресе која се завршава са @opsecsecurity.com, НБС је стигао мејл у коме је измењено једно слово. У њему је наведено да НБС обави плаћање холограмске фолије преко рачуна у пољској *Bank BGZ BNP Paribas SA*, а на рачун компаније „*OpSec Security Limited*“. У овај случај укључен је и Интерпол који покушава да замрзне новчана средства која је НБС уплатила на лажни рачун, док банка чини све да их врати. Такође, српски истражни органи интензивно раде на идентификацији превараната који су напали рачун Народне банке Србије.[34] Нажалост, у тренутку писања овог рада нису пронађене информације о исходу овог случаја.

Такође, у 2016. години регистрован је велики број оштећених привредних субјеката услед фишинг превара. Примећено је да

33) Исто.

34) Blic, *Kako je prevarena nbs izmenili jedno slovo u imejl adresi i ojadili banku za 175.500 evra*, 25.05.2017, Internet, https://www.blic.rs/vesti/drustvo/kako-je-prevarena-nbs-izmenili-jedno-slovo-u-imejl-adresi-i-ojadili-banku-za-175500/b8d362b, 19/07/2018.

извршиоци кривичних дела преваре пресрећу електронске поруке које се размењују између привредних субјеката са територије Републике Србије са пословним партнерима у иностранству. Након компромитовања комуникације, извршиоци шаљу лажну поруку преко већ познатог и уобичајеног канала комуникације (пошто су претходно остварили приступ серверу за електронску пошту), или отварају нове лажне налоге за електронску пошту где се у односу на прави електронски налог који користи страна компанија мењају најчешће словни или бројчани карактери, са циљем да лажни налог подсећа на прави (пример: налог pal@pas.com након измене слова л у број 1 у називу адресе изгледа идентично као права адреса и разлика је тешко уочљива – pa1@pas.com). Овакве измене још теже су уочљиве уколико се комуникација са пословним партнерима одвија свакодневно, а извршиоци ових кривичних дела претходно направе и лажне тј. фишинг интернет странице правних лица у иностранству које су идентичне са правом интернет презентацијом нпр. као што је http://www.example.com у http://www.exmple.com или http://www.evample.com, а ту грешку просечан корисник интернет мреже не може уочити. Злоупотребом комуникације извршиоци кривичних дела лажно се представљају у име стране компаније са којом правни субјекат из наше државе већ има пословну сарадњу и након уговореног посла у преварним порукама одмах након легитимно прослеђене поруке од стране легитимне компаније у којој се налазе инструкције за уплату, шаљу нове поруке са измењеним диспозицијама за плаћање (IBAN број). На описани начин привредни субјекти доводе у заблуду да власницима рачуна који су наведени у тим инструкцијама, а који су заправо извршиоци кривичног дела, уплате новац на своју штету. Имајући у виду да се ради о електронском трансферу новца, извршиоци кривичног дела новац подижу у иностранству веома брзо, понекад и у року од 24 часа. За то време, оштећено предузеће је у убеђењу да је уплатило новац страној компанији, а страна компанија чека уплату за нпр. одређену робу. Да су преварени оштећени сазнају тек након што контактирају страну компанију да питају зашто роба није стигла на време. У просеку, преваре се откривају од стране оштећених тек након три до шест радних дана, што је за учиниоце кривичних дела сасвим довољно да новац у иностранству подигну са рачуна. До сада је утврђено да је дошло до имовинске штете у износу од преко 1.000.000 евра, на штету више десетина привредних субјеката из Републике Србије, каже се у саопштењу МУП и додаје да су наведеним радњама извршилаца кривичног дела преваре највише угрожена мала и средња предузећа с територије Републике Србије[35].

35) Mojnovisad.com, *MUP upozorava: Ovako hakeri varaju firme u Srbiji*, 11.07.2016, Internet,

Једна од најновијих фишинг превара у Републици Србији подразумевала је да на мејл жртве стигне мејл (написан лошим српским језиком и правописним грешкама) са адресе извесне госпође *Celine Joubert*, а у мејлу се жртви саопштава да је случајно изабрана. Преваранти у мејлу наводе да је та жена болесна од рака и да је одлучила да наследство од скоро 900 хиљада евра остави некој насумично одабраној особи. Потом се тражи да је жртва што пре контактира на одређени мејл, а уколико то учини, добија одговор да је потребно обратити се „нотару" преко остављеног мејла. Преваранти су чак у мејлу слали и фотографију своје породице као доказ искрености. Када се жртва јави лажном нотару преко остављеног мејла, нотар јој објашњава да је он заправо адвокат и да ће на рачун жртве „сигурно лећи" обећани износ. Као и код других облика фишинг превара, од жртве се тражи да достави своје личне податке (име, презиме, адресу, број банковног рачуна и слично). На крају, „адвокат" обавештава жртву да ће новац да буде уплаћен на њен рачун, уколико жртва уплатни такозвану „даровницу" од скоро 500 евра, што би наводно био једини трошак жртве. Више грађана Србије било је преварено на овај начин.[36]

Једна од последњих у низу фишинг превара догодила се у јуну 2018. године, када је један грађанин из Београда био жртва скупе фишинг преваре. Наиме, средином маја је на његов мобилни телефон од стране рођака из Русије стигла заражена смс-порука. Када је жртва отворила поруку, поједине апликације на мобилном телефону су престале да раде, а неке су чак и избрисане. Пошто поруку није успео да обрише, искључио је телефон, а након неколико сати схватио је да уопште не може да га користи. Рођак је тврдио да му ништа није послао. Након што је жртва позвала оператера (компанију Теленор), испоставило се да је са његовог телефона послан енроман број смс порука (чак 733) на бројеве са руским позивним бројем, и то у року од два часа, у размаку од три до четири секунде. Телефонски рачун је износио преко 15 хиљада динара, а приговори телефонском оператеру нису уродили плодом. Испоставило се да је корисник отворио садржај из злонамерног смс-а и покренуо инсталацију апликације која је проузроковала слање великог броја смс-порука.[37]

---

http://www.mojnovisad.com/vesti/mup-upozorava-ovako-hakeri-varaju-firme-u-srbiji-id10488.html, 19/07/2018.

36) Blic, *Nova internet prevara stigla u Srbiju "Nudim nasledstvo od 850.000 evra, samo treba da...*", 28.09.2017, Internet, https://www.blic.rs/vesti/hronika/nova-internet-prevara-stigla-u-srbiju-nudim-nasledstvo-od-850000-evra-samo-treba-da/wd54ydl, 19/07/2018.

37) Večernje novosti, *Opasan ruski virus: Beograđanin duguje 15.000 dinara posle ovog SMS-a*, 11.06.2018, http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:732268-OPASAN-RUSKI-VIRUS-Beogradjanin-duguje-15000-dinara-posle-ovog-SMS-a, 19/07/2018.

Имајући у виду наведено, пожељно би било навести одређене *мере заштите од фишинг напада*, које би биле од користи не само грађанима и привредним субјектима, већ и државним институцијама.

Пре свега, препоручљиво би било да прималац потенцијалног фишинг мејла пажљиво провери мејл адресу пошиљаоца и утврди да ли она има макар мале недостатке који су, заправо, главни индикатор потенцијалне преваре. Уколико отвори мејл који је добијен, прималац би требало да провери адресу веб-сајта на који је усмерен. Даље, никад не би требало одговарати на електронске поруке које траже достављање неких личних података, поготово уколико се у мејлу тражи да се оне на било који начин потврде или ажурирају. Нарочито не треба позивати број телефона, уколико је он наведен у сумњивом мејлу. У овом случају, потенцијална жртва фишинг напада би требала да телефонски позове пошиљаоца и провери аутентичност мејла. Треће, примери су показали да је доста наших грађана имало проблема јер су „кликнули" на линк (везу) која је остављена у сумњивом мејлу. У оваквом случају не би требало „кликтати" на остављени линк, већ би било пожељно такозвану URL адресу откуцати у браузеру (прегледачу), или дату веб локацију треба посетити уз помоћ омиљених локација. Четврто, добар начин за избегавање потенцијалних фишинг напада је и избегавање остављања личних података у мејловима који се шаљу. Пето, грађани и привредници треба да буду веома опрезни и у погледу избора компанија са којима послују. Препоручљиво је да се послује са привредним субјектима који су препознатљиви на тржишту по квалитету услуга које пружају, поготово уколико постоји изјава о приватности, којом дати привредни субјект наводи да личне податке пошиљаоца неће прослеђивати другим физичким или правним лицима. Шесто, уколико се врше интернет куповине, пожељно је користити кредитне картице са ниским кредитним ограничењем, јер се тако смањују потенцијалне штетне последице. Посебно је значајно, у случају било какве сумње у веродостојност трансакције, проверити банчине извештаје или изводе са кредитних картица и у случају потребе контактирати банку.

Наравно, фишинг нападе немогуће је у потпуности спречити, без обзира на многобројне корисне савете или софтверска решења (спам филтери и слично). Али, уз адекватну едукацију и повећање безбедносне културе (у чему доста заостајемо за развијеним земљама), праћену одговарајућим софтверима за заштиту од нежељених порука, могуће је ову појаву свести у разумне оквире.

На крају, с обзиром на опасност и велике штете од фишинг превара, од великог значаја би било доношење посебног закона, који би детаљније уредио ову област, као и пооштравање постојећих санкција за овај вид преваре. У томе би у великој мери помогла законодавна решења и богата искуства из САД и одређеног броја других земаља које су донеле посебне законе у овој области.

ЛИТЕРАТУРА

Вилић Вида, *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета* (докторска дисертација), Ниш, 2016.

Домазет Синиша, Скакавац Здравко, „Скандал „Кембриџ Аналитика“-нови изазов у заштити података о личности?“, *Српска политичка мисао*, Институт за политичке студије, Београд, бр. 2/2018.

Ђукић Анђелија, „Крађа идентитета-облици, карактеристике и распрострањеност”, *Војно дело*, Министарство одбране, бр. 03/2017.

Закон о електронској трговини, *Сл. гласник Републике Србије*, бр. 41/2009 и 95/2013.

Кривични законик Републике Србије, *Сл. гласник Републике Србије*, бр. 85/2005, 88/2005 –испр. 107/2005 - испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 и 94/2016).

Петровић Слободан, *Компјутерски криминал*, Војноиздавачки завод, Београд, 2004.

Урошевић Владимир, Ивановић Звонимир, Уљанов Сергеј, *Мач у world wide web-у (изазови високотехнолошког криминала)*, Eternal mix, Београд, 2012.

BBB News, *Newly Identified Phishing Attack Targeting Small Businesses*, 20.07.2018, Internet, https://www.bbbwminews.org/single-post/2017/07/20/Newly-Identified-Phishing-Attack-Targeting-Small Businesses, 16/07/2018.

BBC, *Google Docs users hit by phishing scam*, 04.05.2017, Internet, https://www.bbc.co.uk/news/business-39798022, 16/07/2018.

Blic, *Kako je prevarena nbs izmenili jedno slovo u imejl adresi i ojadili banku za 175.500 evra*, 25.05.2017, Internet, https://www.blic.rs/vesti/drustvo/kako-je-prevarena-nbs-izmenili-jedno-slovo-u-imejl-adresi-i-ojadili-banku-za-175500/b8d362b, 19/07/2018.

Blic, *Nova internet prevara stigla u Srbiju "Nudim nasledstvo od 850.000 evra, samo treba da...*", 28.09.2017, Internet, https://www.blic.rs/vesti/hronika/nova-internet-prevara-stigla-u-srbiju-nudim-nasledstvo-od-850000-evra-samo-treba-da/wd54ydl, 19/07/2018.

Darya Gudkova, Maria Vergelis, Tatyana Shcherbakova, Nadezhda Demidova, *Spam and phishing in 2017 on February 15, 2018. 10:00 am*, *Securelist. 15.02.2018,* Internet, https://securelist.com/spam-and-phishing-in-2017/83833, 15/07/2018.

European Union Agency for Network and Information Security (ENISA). *ENISA Threat Landscape Report 2017, 15 Top Cyber-Threats and Trends*, Internet, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, 17/07/2018.

Gulf Times, *Qatar faced 93,570 phishing attacks in first quarter of 2017*, 12.03.2017, Internet, http://www.gulf-times.com/story/547784/Qatar-faced-93-570-phishing-attacks-in-first-quart, 16/07/2018.

Gunter Ollmann, *The Phishing Guide (Understanding & Preventing Phishing Attacks)*, NGSSoftware Insight Security Research, United Kingdom, 2004, Internet: https://www.nccgroup.trust/uk/our-research/the-phishing-guide-understanding-preventing-phishing-attacks/, 14/07/2018

Infosecurity, *Airbnb Customers Targeted with Phishing Scam*, 04.05.2018, Internet, https://www.infosecurity-magazine.com/news/airbnb-customers-targeted-with/, 18/07/2018.

KasperskyLab, *GDPR bustle: Even scammers have new privacy policies*, 29.05.2018., Internet, https://www.kaspersky.com/blog/apple-gdpr-phishing/22517/, 18/07/2018.

Kimkomando, *Amazon Prime Day phishing scam spreading now!*, 21.08.2017, Internet, https://www.komando.com/happening-now/415020/amazon-prime-day-phishing-scam-spreading-now, 16/07/2018.

Mojnovisad.com, *MUP upozorava: Ovako hakeri varaju firme u Srbiji*, 11.07.2016, Internet, http://www.mojnovisad.com/vesti/mup-upozorava-ovako-hakeri-varaju-firme-u-srbiji-id10488.html, 19/07/2018.

Pysis.net, *WannaCry Exposes Extent of Cyber Crime Threat to Small Business*, 12.06.2017, Internet, https://www.pisys.net/blog/wannacry-exposes-extent-of-cyber-crime-threat-to-small-business.asp, 16/07/2018.

Rasha Almahroos, "Phishing for the Answer: Recent Developments in Combating Phishing", *A Journal of Law and Policy for the Information Society*, Ohio State University, Moritz College of Law, United States, бр. 3/2007.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, стр. 1–88.

SC Media, *Nigeria-based BEC scams pulling in millions, SecureWorks report*, 05.08.2016, Internet, https://www.scmagazine.com/nigeria-based-bec-scams-pulling-in-millions-secureworks-report/article/528085/, 16/07/2018.

Scot Graydon, "Phishing and Pharming: The New Evolution of Identity Theft", *Consumer Financial Law quarterly Report*, бр. 60/2006.

Small Business Trends *W-2 Phishing Scam Threatening Small Business After Tax Day*, 02.05.2017, Internet, https://smallbiztrends.com/2017/05/w-2-phishing-scam-small-business.html, 16/07/2018.

The Guardian, *'Petya' ransomware attack: what is it and how can it be stopped?*, 28.06.2017, Internet, https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how, 16/07/2018.

TVN1, *Tokom Mundijala sprečeno 25 miliona sajber napada*, http://rs.n1info.com/a404278/Svet/Svet/Tokom-Mundijala-sprece-no-25-miliona-sajber-napada.html, Internet, 16/07/2018.

Večernje novosti, *Opasan ruski virus: Beograđanin duguje 15.000 dinara posle ovog SMS-a*, 11.06.2018, http://www.novosti.rs/vesti/naslovna/hronika/aktuelno.291.html:732268-OPASAN-RUSKI-VIRUS-Beogradjanin-duguje-15000-dinara-posle-ovog-SMS-a, 19/07/2018.

Sinisa Domazet, Zdravko Skakavac

"PHISHING" – A CHALLENGE IN THE PROTECTION OF SECURITY OF INTERNET USER'S DATA

Resume

In this scientific work we analyzed one form of cyber crime, which is called a phishing ("fishing"). The study found that the number of phishing scam is increasing from year to year, with severe damage. Forms and methods of execution of this type of fraud have evolved over time and become more sophisticated and therefore more difficult to detect. It was shown that phishing attacks affected not only the citizens, but also businesses and important state institutions. The paper presents examples of phishing attacks in the world and in the Republic of Serbia. The analysis showed that the Republic of Serbia are increasingly threatened due to phishing attacks and that there is no *lex specialis* regulating this issue. It has been determined that it is necessary to take a number of preventive measures to prevent theft of private data and other important information. This means increased caution when emails, carefully reading their contents, avoiding the "clicking" on suspicious links which activates the malicious software, increased caution in electronic commerce and with use of credit cards, and other relevant measures. Citizens and businesses should be very careful in the choice of companies with which they do business. It is advisable to do business with companies that are recognized in the market by the quality of services provided, especially if there is a privacy statement, in which the undertaking states that personal data will not be passed on from sender to other persons or entities. In cases of internet trade, it is preferable to use a credit card with a low credit limit, because it reduce the potential for harmful consequences. It is particularly important to check the bank's reports or copies of credit card in the case of any doubt regarding the authenticity of the transaction. The paper points out the need to enact a special law that would regulate the phishing scams, as well as stricter penal policy. Legislative solutions and rich experience in the USA and a number of other countries that have enacted specific legislation in this area would be of great help. The research used normative methods and legal and logical methods of induction and deduction.

Keywords: law, European Union, security, phishing, internet

* Овај рад је примљен 27. октобра 2018. године, а прихваћен на састанку Редакције 7. марта 2019. године.