Проф. др Младен МИЛОШЕВИЋ[*]
Проф. др Ненад ПУТНИК[**]
Факултет безбедности Универзитета у Београду

ДОИ: 10.5937/bezbednost1902068M
УДК: 343.533:004
Прегледни научни рад
Примљен: 30. 5. 2019. године
Датум прихватања: 4. 6. 2019. године

Специфичности извршења кривичног дела преваре уз коришћење информационо-комуникационих технологија

***Апстракт**: Посматрано из историјске перспективе, паралелно са развојем информационо-комуникационих технологија (ИКТ) развијају се и начини њихове злоупотребе. Злонамерни актери континуирано проналазе нове методе за злоупотребу ових технологија које су засноване на рањивостима ИКТ система, било да је реч о техничким или рањивостима везаним за људски фактор.*

У раду су описани феномени тзв. социјалног инжењеринга и фишинга, као начина извршења кривичних дела преваре и рачунарске преваре, којима се незаконито прикупљају и користе подаци корисника ИКТ система како би се они довели у заблуду или одржали у њој и услед тога поступили на штету сопствене или туђе имовине, уз намеру стицања противправне имовинске користи од стране учиниоца. Савремени фишинг напади су веома софистицирани, прилагођени потенцијалној жртви и усклађени са њеним афинитетима. Прикупљање информација о потенцијалној жртви најчешће се спроводи путем друштвених мрежа. Стога је у раду описан процес планирања преварних радњи и објашњене су две најзаступљеније технике прикупљања података – путем друштвених мрежа и путем нелегалног преузимања контроле над рутером жртве.

[*] milosevic@fb.bg.ac.rs
[**] nputnik@fb.bg.ac.rs

Посебан акценат је стављен на кривичноправни третман ових феномена у законодавству Републике Србије као и на појмовно разјашњење терминолошких недоумица у вези са преварним радњама у српском и англосаксонском језику. Аутори представљају хетерогене облике испољавања социјалног инжењеринга и фишинга у ИКТ системима, тј. сајбер простору, и разматрају да ли се и у којим случајевима њиховим вршењем испуњавају законска обележја поменутих кривичних дела.

***Кључне речи**: високотехнолошки криминалитет, кривично дело преваре, кривично дело рачунарске преваре, социјални инжењеринг, фишинг, сајбер простор.*

Увод

Технике обмањивања старе су колико и сам људски род. Међутим, са развојем савремених информационо-комуникационих технологија (ИКТ) и прогресивном информатизацијом друштва појавиле су се нове, специфичне, преварне технике које имају за циљ обмањивање корисника ових технологија. За те технике се у српском језику користи појам *преварне радње*, док се у англосаксонском говорном подручју користи појам *социјални инжењеринг*.

Сајбер напад који има за циљ остваривање неауторизованог приступа заштићеном ИКТ систему није једноставно спровести. Самом чину извршења напада мора претходити детаљно планирање акције. Може се рећи да је то, у суштини, дуготрајан процес, који се одвија кроз одређене фазе.

Неки од ових корака су аутоматизовани и извршавају се коришћењем малициозних програма или других инструмената који се могу лако набавити у глобалној мрежи.

Други кораци пак захтевају коришћење преварних радњи (у реалном или виртуелном простору) које су усмерене ка лицима која опслужују информационе системе, са циљем откривања њихових приступних креденцијала неопходних нападачу за неопажен приступ систему који је на мети напада.

Професионални нападачи приликом планирања и извршења напада најчешће користе комбиновани приступ који подразумева примену софистицираних и персонализованих информатич-

ких алата, с једне стране, и преварних радњи, с друге стране. Ефекти софистицираних алата су тешко опажљиви од стране стручњака на пољу сајбер безбедности (Мандић, Путник, Милошевић, 2017).

На теоријској равни се може разликовати пет фаза сајбер напада: препознавање и преоперативни надзор; анализа (*scanning*); приступ; одржавање приступа и прикривање трагова (Skoudis, 2002). У првој фази нападач се детаљно упознаје са информацијама које ће му олакшати приступ информационом систему који намерава да нападне. Преварне технике показују се као неопходне већ у овој фази, како би се од особе блиске систему добиле осетљиве информације (као што су бројеви телефона, органиграми организације, подаци о приступним налозима и лозинкама итд.).

Појам, врсте и карактеристике преварних радњи у сајбер простору

Сада већ давне 1997. године скован је појам *социјални инжењеринг*, под којим је подразумеван вид манипулације појединцима како би се они навели да испуне одређене захтеве нападача који су, по правилу, у супротности са процедуралним, правним и/или етичким нормама.

Иако се некоме може чинити да појам социјални инжењеринг није научно етаблиран, приметно је да је он у англосаксонском говорном подручју у све чешћој употреби, и у научној и у стручној литератури. Он се користи увек када је потребно указати на манипулацију људима, како у физичком тако и у виртуелном простору, и под њега се подводе специфичне технике обмањивања корисника информационо-комуникационих система, као што су фишинг, вишинг и друге. У том смислу, можемо тврдити да је овај појам у стручној и научној литератури временом стекао свој садржај и опсег, те да је данас попримио прилично јасну и одређену денотацију (Мандић, Путник, Милошевић, 2017).

Израз социјални инжењеринг данас се најчешће користи да опише технику напада на штићени информациони систем, где нападач покушава да путем комуникације наведе (убеди) жртву да прекрши безбедносне норме или процедуре и открије податке за приступ циљаном систему, а да притом не примети да је измани-

пулисана. Према томе, социјални инжењеринг има за циљ прикупљање корисних информација за приступ мрежи или систему жртве − оних информација које нису лако доступне сајбер нападима техничког типа (Путник, 2009). Нарочито се примењује у случајевима када је информациони систем жртве заштићен јаким безбедносним мерама.

Социјални инжењеринг се заснива на констатацији да људски фактор, као централни елемент у архитектури информационе безбедности (не постоје рачунари или мреже који се не заснивају на учешћу човека), уједно представља и њену најслабију компоненту. С обзиром на то да је човек неопходан за рад рачунара, јасно је да слабост овог елемента информационе безбедности јесте и извор универзалне рањивости информационих система: онај ко има приступ било којем делу система, физички или електронски, представља потенцијалну претњу за безбедност тог система (Rittinghouse, Hancock, 2003).

За разлику од осталих напада на рачунаре, социјални инжењеринг не мора да се односи на технолошку манипулацију и коришћење рањивости хардвера или софтвера и, поред тога, не захтева посебне техничке вештине и знања. Ова врста напада експлоатише људске слабости, као што су немарност или жеља за кооперативношћу, како би се добио приступ легитимним документима који се налазе у дигиталном формату (Shinder, 2002). Управо због тога је најтеже одбранити се од напада социјалним инжењерингом, јер га не могу зауставити самостално ни хардвер ни софтвер (Mathew, 2004).

Основни циљ социјалног инжењеринга јесте да се задобије неовлашћен приступ рачунарским системима или осетљивим информацијама. Након што је добио приступ жељеној информацији, нападач је може употребити за планирање или извршење других напада у физичком или виртуелном свету. Лица која користе социјални инжењеринг најчешће циљају на организације које располажу великим базама података у дигиталном формату, као што су провајдери телефонских услуга, мултинационалне компаније, финансијски ентитети, болнице и војска (Janczewski, Colarik, 2008).

Постоје три основна начина извршења социјалног инжењеринга: контактом (личним контактом, телефоном, преко друштвених мрежа), без контакта (употребом малициозног софтвера, пос-

тављањем интернет адресе, подметањем преносног меморијског медијума) и приступом који комбинује претходно наведене (Мандић, Путник, Милошевић, 2017).

Једна од најзаступљенијих техника социјалног инжењеринга, која се углавном извршава без контакта (најчешће преко електронске поште и телефоном), позната је под именом *фишинг* (енг. *phishing*). Реч фишинг означава намерно погрешно написану реч пецање (енг. *fishing*). Највероватније потиче од израза *password harvesting fishing* (пецање на плантажама лозинки). Фишинг је облик социјалног инжењеринга у којем нападач покушава да преваром дође до поверљивих информација од жртве, лажно се представљајући као трећа страна од поверења (Jagatic et al., 2005).

Термин фишинг користи се да опише поступак илегалног прикупљања осетљивих информација, добијених обманом у сајбер простору, при којем се нападач представља као неко вредан поверења ко има право и потребу да таквим информацијама располаже. Традиционални фишинг подразумева стварање лажних интернет страница које су визуелно идентичне оригиналима, а чија је сврха преузимање поверљивих личних података. У такве податке убрајају се најчешће корисничко име и лозинка, али и ПИН код банкарских картица и слично (Мандић, Путник, Милошевић, 2017).

Фишинг сајтови су екстремно софистицирани и обично их је тешко разликовати од правог сајта, сем по адреси на којој се налазе. Корисницима линкови до ових страница могу бити подметнути путем електронске поште, друштвених мрежа, форума – практично кроз све облике комуникације на интернету.

Напад најчешће започиње тако што нападач настоји да усмери жртву ка одређеној веб-страници, дизајнираној тако да имитира визуелни идентитет легитимне организације. Не сумњајући у аутентичност веб-странице, жртва на њој оставља властите поверљиве податке. У следећем кораку нападач користи прикупљене личне податке жртве, тј. преузима њен идентитет како би извршио незаконите финансијске трансакције. На тај начин жртве могу претрпети значајне финансијске губитке или, у озбиљнијим случајевима, чак и губитак сопственог „електронског идентитета“ који бива искоришћен за криминалне циљеве (Мандић, Путник, Милошевић, 2017).

Напади фишингом се ослањају на комбинацију техничке преваре и праксе социјалног инжењеринга. У већини случајева нападач мора убедити жртву да намерно изврши низ радњи које ће му обезбедити приступ поверљивим информацијама (Ollmann, 2004).

Ако томе додамо да је крајњи циљ социјалног инжењеринга долажење до одређене информације, што је и циљ фишинга, увиђамо да постоји и сличност између ова два појма. Суштинска разлика није у циљу коме се тежи, већ у томе што социјални инжењеринг, користећи разне технике, наводи мету напада да уради нешто што иначе не би урадила, односно, у случају фишинга, да посети лажни сајт и на тај начин компромитује своје информације (Мандић, Путник, Милошевић, 2017).

Један од нових појавних облика фишинга је *директни фишинг* (*spear phishing*), где се циљано напада тачно и увек унапред дефинисана мета. Јасно је да је та техника много опаснија од традиционалног фишинга јер се унапред дефинише мета напада, што значи да унапред дефинисан циљ условљава и технику напада.

Кривичноправни оквир

Кривичноправни оквир за супротстављање тзв. сајбер криминалитету у Србији почео је да се изграђује доношењем Закона о изменама и допунама Кривичног закона Србије, 2003. године (ЗИДКЗ, 2003), када је кривично законодавство измењено увођењем кривичних дела против безбедности рачунарских података, систематизованих у засебну главу закона. Пресудан утицај на наше законодавство имале су Конвенција Савета Европе о сајбер криминалу, усвојена 2001. године у Будимпешти (ступила на снагу 2004. године), и њен Додатни протокол о кажњавању аката расизма и ксенофобије учињених путем компјутерских система из 2003. године, коју је Државна заједница Србије и Црне Горе потписала 2005. године.

Пре доношења те конвенције, у периоду од 1989. до 2000. године, усвојен је низ инструмената међународног права у области криминалитета везаног за компјутере (Препорука Савета Европе о криминалитету везаном за компјутере, 1989; Резолуција Уједињених нација о компјутерском криминалитету, 1990; Резолуци-

ја Међународног удружења за кривично право везана за компјутерски криминалитет, 1992; Директива Европске уније о електронском пословању из 2000. године, и др.), али је неспорно да је тек њено ступање на снагу означило прекретницу у борби против ове савремене и сложене форме криминалног деловања (Стојановић, Делић, 2015: 283).

Иако се уочава извесна временска дискрепанца између ратификације Конвенције и мењања домаћег кривичног законодавства, наша држава је углавном на адекватан начин испунила обавезе преузете усвајањем овог међународноправног акта. Кривични законик Србије из 2005. године (КЗ, 2005) задржао је посебну главу (Глава 27) под називом „Кривична дела против безбедности рачунарских података“ уз одређене измене у односу на одредбе претходно важећег кривичног закона.

Ипак, вреди нагласити да је појам високотехнолошког криминала у нашем законодавству шири од опсега кривичних дела против безбедности рачунарских података. Према члану 2 став 1 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала ова врста криминалитета обухвата вршење кривичних дела код који се као „објекат или средство извршења кривичних дела јављају рачунари, рачунарски системи, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику“ (Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала, 2005). Изменама и допунама закона из 2009. године прецизирана су кривична дела за чије се откривање, гоњење и суђење примењују одредбе овог прописа, чиме је, барем у законском смислу, етаблирано значење термина високотехнолошки криминал (члан 3 Закона о организацији и надлежности државних органа за борбу против високотехнолошког криминала).

Кривично дело рачунарске преваре уведено је поменутим изменама и допунама из 2003. године и у готово истоветном облику је опстало до данас. Законски опис из члана 186г Кривичног закона Србије (КЗС, 1977) практично је истоветан са оним из члана 301 Кривичног законика (КЗ, 2005) осим разлике у новчаним износима штете који чине квалификаторне околности (тежи и најтежи облик кривичног дела).

Дело из члана 301 КЗ има основни, два квалификована и привилеговани облик. Биће основног облика кривичног дела садржи радњу и последицу, а имплицитно су садржани средство извршења и објекат радње као објективна обележја, док субјективни супстрат дела чине умишљај и одговарајућа намера. Постојање намере као субјективног обележја одређује да је дело могуће учинити једино са директним умишљајем, док је евентуални умишљај искључен.

Радња основног облика састоји се у предузимању делатности (комисивних или омисивних) којима се прикривају или лажно приказују подаци. Законодавац експлицитно наводи две радње – уношење нетачног податка и избегавање да се унесе тачан податак, али додаје и широку формулацију „или на други начин лажно прикаже или прикрије податак“, што представља правни стандард и омогућава релативно екстензивно тумачење.

Последица кривичног дела састоји се у утицању на резултат процеса електронске обраде и преноса података. Делатности извршиоца треба да доведу до одређене промене у аутоматској обради и преносу која се испољава у произвођењу другачијег резултата обраде у односу на очекивани, то јест резултат који би наступио да су унети параметри били аутентични. За постојање дела се захтева и наступање имовинске штете по другог, што представља за нијансу другачију формулацију у односу на кривично дело преваре из члана 208 КЗ („и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини“).

Овде се може поставити питање да ли имовинска штета представља објективни услов инкриминације или је, заједно са утицањем на резултат електронске обраде и преноса података, последица кривичног дела. У првом случају имовинска штета не би морала да буде обухваћена умишљајем учиниоца, те ово представља и важно фактичко питање. С обзиром да је рачунарска превара специјалан случај преваре, питање треба решавати уз узимање у обзир законског описа дела из члана 208 КЗ.

Према мишљењу заступљеном у литератури, код кривичног дела преваре штета по имовину другог треба заиста да наступи како би дело било довршено (Стојановић, 2012; Ђорђевић, 2014; Стојановић, Делић, 2015). На основу тога закључујемо да би и формулацију законодавца код кривичног дела рачунарске прева-

ре било исправно тумачити тако да наступање имовинске штете представља последицу кривичног дела, те је њено наступање нужно да би се дело сматрало свршеним, а умишљај учиниоца мора да обухвати и свест о наступању имовинске штете.

Дакле, кривично дело рачунарске преваре је довршено када се предузимањем радње оствари такав утицај на резултат електронске обраде и преноса података да услед њега наступи имовинска штета по другог.

Овде се основано поставља питање разликовања објективних обележја рачунарске преваре од основног облика дела из члана 208 КЗ. Код „класичног" кривичног дела преваре извршилац лажним приказивањем или прикривањем чињеница пасивног субјекта доводи или одржава у заблуди и тиме га наводи да нешто учини или не учини на штету своје или туђе имовине. Дакле, пасивни субјект је истовремено и предмет радње, то јест објект кривичног дела.

С друге стране, биће кривичног дела рачунарске преваре конструисано је тако да пасивни субјект није у потпуности подударан са предметом радње, јер се радња врши у оквиру рачунарске обраде података, а последица наступа како на самом процесу обраде и преноса података тако и на имовини пасивног субјекта. Радња се првенствено предузима на рачунару или рачунарској мрежи, а имовина пасивног субјекта бива оштећена због промењеног резултата процеса електронске обраде и преноса података који се одвија у оквиру система или мреже.

Ипак, у пракси се разликовање та два кривична дела може показати као тешко. Примера ради, кривично дело преваре може се извршити посредством фалсификоване исправе или лажног представљања, па исто тако и коришћењем рачунара. Питање је да ли се рачунарском преваром може назвати сваки случај преваре у ком се као средство извршења користе рачунари, рачунарски системи или мреже.

Нама се чини да је одговор негативан. Наиме, рачунарска превара свакако подразумева да су рачунари или рачунарске мреже средство извршења кривичног дела и то обележје је неспорно. Међутим, суштинска разлика у односу на дело из члана 208 КЗ јесте то што се рачунари или рачунарске мреже, односно свака аутоматизована електронска обрада или пренос података, појављују

и као објект радње, а не само као средство извршења. Суштински, кривично дело преваре би постојало када би се као средство извршења користио рачунар, под условом да предмет радње није било утицање на електронску обраду и пренос података већ стварање погрешне представе код оштећеног услед које он нешто предузима на штету своје или туђе имовине.

У том смислу, слање мејлова који би садржали превару познату као „нигеријска“ (један од најпознатијих видова фишинга) услед којих би потенцијална жртва била наведена да себи нанесе имовинску штету због лажних чињеница изнетих у тексту електронске поруке које су је навеле да поступи противно својим материјалним интересима, представљало би кривично дело из члана 208 КЗ, без обзира што је изведено уз помоћ рачунара и рачунарске мреже. Треба имати у виду да ширина појма „високотехнолошки криминал“ омогућава да се и то дело открива, гони и суди сходно Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала (члан 3 Закона), али оно свакако остаје квалификовано као дело преваре, а не рачунарске преваре.

Тако, можемо закључити да бројне интернет преваре често не могу да се квалификују као рачунарске преваре, већ сходно одредби члана 208 КЗ, јер не постоји засебно кривично дело интернет преваре, различито од дела из члана 301 и дела из члана 208 КЗ (Вилић, 2016; Мирић, 2018).

Рачунарска превара постојала би у случају да извршилац успе да утиче на аутоматску обраду података тако да она пружи лажан резултат. Уколико бисмо отварањем интернет везе (линка) дошли на лажну страницу банке, изабрали опцију за плаћање преко интернет мреже и тиме уплатили новац на рачун на који нисмо желели, јер су подаци о трансакцији измењени, онда би била реч о рачунарској превари (традиционални начин извршења фишинга).

Вреди напоменути да је кривично дело преваре уз коришћење информационо-комуникационих технологија, имајући у виду хетерогене појавне облике, могуће подвести и под друге правне квалификације, које такође представљају специјалне случајеве преваре, али их је законодавац уздигао на ранг посебних кривичних дела. Ту мислимо на кривична дела: превара у обављању привредне делатности (члан 223 КЗ); превара у осигурању (члан 223а

КЗ) и превара у служби (члан 363 КЗ). Свако од наведених кривичних дела може се извести тако да средство извршења буду информационо-комуникационе технологије, тако да, феноменолошки гледано, коришћење информационо-комуникационих технологија за вршење преварних радњи може да задобије различите кривичноправне облике, односно правне квалификације.

Посебно треба размотрити и могућност да правно лице буде извршилац неког од кривичних дела преваре (општег из 208 или наведених посебних случајева преваре, укључујући рачунарску). Међутим, примена Закона о одговорности правних лица за кривична дела у Србији (Закон о одговорности правних лица за кривична дела, 2008) од његовог доношења до данас је била изузетно ретка. Основ одговорности правног лица за кривично дело могао би бити испуњен приликом предузимања радње неког од наведених кривичних дела, јер је лако замисливо да се радња врши у склопу обављања послова одговорног лица уз постојање намере да се противправна имовинска корист стекне, макар и делимично, и за правно лице (Милошевић, 2012; Милошевић, 2012а; Милошевић, Симовић, 2018).

Субјективни елемент кривичног дела рачунарске преваре осим директног умишљаја, који подразумева свест и вољу о свим законским обележјима кривичног дела, обухвата и намеру да се „себи или другом стекне противправна имовинска корист“ (члан 301 КЗ). Привилеговани облик дела постоји када учинилац има искључиву намеру да другоме нанесе имовинску штету. Ту, дакле, извршилац тежи да другог оштети, а не и да себи или неком трећем лицу прибави имовинску корист. У том случају дело је довршено без обзира на то да ли је штета наступила или не, јер је она део субјективног елемента овог облика кривичног дела, а не и његово објективно обележје (Стојановић, 2012).

Тежи и најтежи облик се од основног облика не разликују по субјективном елементу, већ по објективном обележју – тежини последице, односно висини имовинске штете која је наступила. Код тежег облика износ штете треба да пређе 450.000 динара, док код најтежег он износи преко 1.500.000 динара.

Код основног облика запрећена је новчана казна или затвор до три године, код првог тежег облика казна је од једне до осам година затвора, док је код најтежег облика она прописана у

распону од две до десет година. Лакши облик кривичног дела се кажњава новчаном казном или затвором до шест месеци (Мандић, Путник, Милошевић, 2017).

Могућности откривања идентитета жртве на друштвеним мрежама у циљу прикупљања података за извршење директног фишинг напада

Посматрано из феноменолошке перспективе, можемо приметити да се континуирано изналазе нови начини за извршење преварних радњи које се одвијају уз коришћење информационо-комуникационих технологија. Међу разноврсним појавним облицима тих радњи фишинг напади су доминантни, превасходно услед своје ефикасности. Један од разлога њихове учинковитости лежи у томе што фишинг мејлови нису униформни већ су специфични, прилагођени потенцијалној жртви и усклађени са њеним афинитетима (политичком, верском, идеолошком и сексуалном оријентацијом, преференцијама и слично).

Злонамерни актери често прикупљају информације о жртви путем друштвених мрежа. Наравно, успех те прикупљачке активности зависи од више фактора. Један од њих је, свакако, присутност потенцијалне жртве на друштвеним мрежама. Други фактори се тичу присутности жртве у сајбер свету уопште – броја и врста база података у којима су ускладиштени подаци о њој, међусобне повезаности база (њиховог такозваног међусобног „линковања“) као и врста података који су ускладиштени (текст, слика, видео-запис). Успех прикупљања података зависи и од употребљивости оних података којима злонамерни актер иницијално располаже.

У намери да осветле међусобну повезаност тих фактора, те могућности за прикупљање података неопходних за спровођење фишинг напада путем друштвених мрежа, истраживачи једне од најпознатијих компанија за заштиту ИКТ система Касперски лаб (Kaspersky Lab), у фебруару 2019. године спровели су пилот-истраживање. Циљ истраживања је био да се на основу малог броја почетних података, користећи јавно доступне алате за претрагу, на друштвеним мрежама открије идентитет (профил) пет особа

које су пристале да буду предмет обраде података (How cybercriminals harvest information for spear phishing, 2019).

Резултати истраживања су показали да фотографија није најзахвалнији нити најчешћи полазни основ за претраживање (откривање нечијег онлајн идентитета), те да поседовање фотографије потенцијалне жртве тешко да може нападача довести до њеног профила на друштвеној мрежи.

Постоји више апликација које се могу користити за ту намену. На пример, може се користити бесплатни Гуглов (Google) претраживач за претраживање по задатим фотографијама, који постоји и у облику додатка основном веб-претраживачу. Та апликација, дакле, омогућава претрагу на основу задате фотографије. Она, међутим, „упарује“ само оне фотографије које су већ објављене на интернету, па би била бескорисна нападачу који располаже фотографијом жртве (у физичкој или електронској форми) која није претходно објављена и индексирана на интернету.

Постоје и друге апликације и сервиси које се могу користити за ову намену, али они нису бесплатни. У фебруару 2016. године појавила се, тада бесплатна, онлајн платформа Фајндфејс (FindFace). Она је на основу неколико квалитетних фотографија циљане жртве могла брзо да пронађе њене налоге на друштвеним мрежама. Међутим, од 1. септембра 2018. године овај сервис више није доступан обичним корисницима јер су се његови креатори усмерили ка развоју те услуге за потребе државних органа и корпорација. Према наводима креатора сервиса, његове могућности су много веће од онога што је било видљиво у јавно доступној верзији (https://findface.ru/).

Истраживање компаније Касперски је, према томе, показало да је мало вероватно да су криминалци у стању да повежу постојећу фотографију жртве у физичком свету са профилном сликом на друштвеним мрежама, уколико не употребе неки од скупих онлајн сервиса за препознавање лица чије потенцијално коришћење, притом, оставља и форензичке трагове. Па ипак, могућност откривања нечијег идентитета на друштвеним мрежама помоћу задате фотографије не би требало олако одбацити, будући да су криминалци често спремни да улажу финансијска средства и употребе додатне ресурсе, у складу са циљем који желе да постигну.

Претрага на основу имена и презимена, као задатих критеријума, много је успешнија. Проналажење одређене особе која има уобичајено и често име (нпр. Петар Петровић) може да буде тежак задатак, док особу са ретким именом и презименом Гугл проналази прилично брзо (How cybercriminals harvest information for spear phishing, 2019).

Претрага на основу имејл адресе и броја телефона као задатих критеријума такође је прилично успешна, показује истраживање. Значајну помоћ у претраживању могу пружити агрегаторски софтвери, који аутоматски сакупљају потребне податке. Међу њима је најполуларнији Пипл (Pipl), који може пронаћи линкове до корисничких страница на друштвеним мрежама на основу броја телефона или имејл адресе, и дати кратку биографију корисника, укључујући место рођења, студија, и запослења. Према наводима креатора сервиса, Пипл има информације о више од три милијарде људи (https://pipl.com/corp/blog). Истраживачи компаније Касперски су, користећи ову услугу, добили линк за пет од десет учесника експеримента, за најмање један кориснички налог, а у неким случајевима су чак дошли и до онлајн надимка или корисничког имена (How cybercriminals harvest information for spear phishing, 2019).

У рукама сајбер криминалаца свако корисничко име може се искористити за стицање додатних информација о циљаној жртви. Претраживање на основу корисничког имена може се спровести помоћу алата као што су *namechk* (https://namechk.com/) или *knowem* (https://knowem.com/). Први може да пронађе име налога на више од 100 различитих сервиса. Други проверава више од 500 ресурса. Наравно, ако је корисничко име веома често, не постоји гаранција да ће конкретна особа бити пронађена. Па ипак, овакви алати су веома корисни преварантима у сајбер простору. Често су корисници ИК технологија склони да употребљавају само једно корисничко име за личне и корпоративне адресе електронске поште, као и за налоге на друштвеним мрежама, што је свакако непромишљено и потенцијално веома опасно.

Преузимање контроле над рутером као алтернативна техника извршења директног фишинг напада

Фишинг напади се могу заснивати на различитим техникама извршења. Традиционална и најзаступљенија техника, видели смо, подразумева употребу имејл порука за спровођење обмане. Алтернативне технике извршења подразумевају употребу телефона (тзв. „вишинг“, енг. *vishing* – кованица настала спојем речи *voice* и *phishing*) или комбиновање различитих техника (нпр. употреба телефона и аудио-записа који се током разговора пуштају са рачунара). Једна од најновијих техника подразумева тајно преузимање контроле над рутером жртве (његову отмицу).

Преузимање контроле над рутером жртве може се остварити на два начина. Први приступ подразумева злоупотребу фабрички дефинисаних креденцијала (корисничко име и лозинка) за приступ рутеру. Будући да сваки рутер има фабрички дефинисане креденцијале за приступ администраторском панелу рутера, а да већина корисника услед недостатка безбедносне културе те креденцијале не мења приликом инцијалног подешавања уређаја, злонамерни актери могу лако остварити приступ рутеру (Phishing without borders, or why you need to update your router, 2019).

Други приступ подразумева искоришћавање рањивости фирмвера рутера, који омогућава злонамерном актеру да преузме контролу над рутером без икакве лозинке.

Након преузимања рутера, нападач модификује његове поставке. То је мала, неприметна промена која подразумева промену адресе DNS (*Domain Name System*) сервера који рутер користи за решавање имена домена. DNS заправо служи као „именик“ интернета, повезујући IP адресе и домене. Његова функција је да преводи адресу веб-сајта из људски читљивог облика у своју нумеричку IP адресу и да је, након тога, саопшти прегледачу (Šta je DNS i koji je najbrži DNS?, 2018).

У ситуацији када је рутер отет и адресе жртвиног DNS сервера промењене, сви упити са претраживача упућују се на злонамерни DNS сервер који контролише нападач. Због тога злонамерни сервер враћа претраживачу фалсификовану IP адресу, уместо IP адресе сајта који је жртва желела да посети. Притом, жртва не сумња у легитимност странице која је учитана, нити рачунар мо-

же да региструје ову врсту измењене комуникационе трасе. О учинковитости ове технике сведоче скорашњи напади спроведени над корисницима рутера произвођача: D-Link DSL, DSLink 260E, ARG-V4 ADSL, Secutech и Totolink, у Бразилу. Нападачи су искористили безбедносне пропусте у рутерима наведених произвођача, компромитовали уређаје и модификовали њихове DNS поставке. Када би власници отетих рутера покушали да приступе својим интернет банкарским рачунима или сајтовима провајдера, злонамерни DNS сервер под контролом отмичара би их неприметно преусмерио на фишинг странице (које су имитирале легитимне странице бразилских финансијских институција, банака, као и веб-хостинг и клауд провајдера) дизајниране да украду њихове креденцијале (Phishing without borders, or why you need to update your router, 2019).

Закључак

Најновија искуства из области заштите од преварних радњи у сајбер простору сведоче о томе да прикупљање личних и осетљивих података о потенцијалним жртвама не захтева висок ниво техничког знања, као ни приступ сложеним услугама и скупим сервисима за претраживање података. Стога се може очекивати и даље повећање учесталости кривичних дела преваре заснованих на коришћењу информационо-комуникационих технологија, превасходно у домену директних фишинг напада.

Кривичноправна регулатива превара у сајбер простору омогућава адекватно санкционисање учинилаца и пружа правне квалификације под које се могу подвести бројна друштвено опасна дела изведена коришћењем информационо-комуникационих технологија. Ипак, остаје питање да ли је било нужно ограничити законски опис кривичног дела рачунарске преваре на ситуације у којима се као средство извршења и објект радње појављују рачунари и рачунарске мреже, односно процеси електронске обраде и преноса података, или га је требало конструисати тако да се односи на све врсте преварног поступања употребом високих технологија. Уколико се сложимо с ставом да би таква формулација могла да буде сувише уопштена, екстензивна и неодређена, остаје друга могућност – увођење засебног кривичног дела интернет преваре.

Чини нам се ипак, да правно-технички најпогодније решење може да буде јединствена формулација којом би се објединила рачунарска и интернет превара, и поред потенцијалне ширине и мање одређености таквог законског описа. Наиме, верујемо да би се евентуални приговори могли отклонити стварањем прецизне али и флексибилне формулације која би била сачињена у складу са природом ове врсте инкриминисаног понашања. Мислимо да би биће кривичног дела рачунарске преваре, *de lege ferenda*, могло да гласи: ко унесе нетачан податак, пропусти да унесе тачан податак, на други начин лажно прикаже или прикрије податак или коришћењем интернета или сличних платформи информационо-комуникационе технологије, утиче на резултат електронске обраде или преноса података, или доведе или одржава у заблуди друго лице и тиме проузрокује имовинску штету, казниће се...

Наведеном инкриминацијом би се истовремено обухватили случајеви деловања на аутоматску обраду података уношењем или неуношењем података и случајеви интернет превара чији су објект радње корисници информационо-комуникационих технологија, чиме би се пружила потпунија и адекватнија кривичноправна заштита.

Литература

1. Вилић, В. (2016). *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета, докторска дисертација*. Правни факултет Универзитета у Нишу, Ниш.
2. Ђорђевић, Ђ. (2014). *Кривично право – посебни део*. Криминалистичко-полицијска академија, Београд.
3. *Закон о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, Службени гласник Републике Србије бр. 61/05, 104/09.
4. *Закон о потврђивању Конвенције о високотехнолошком криминалу*, Службени гласник Републике Србије број 19/09
5. *Закон о потврђивању Додатног протокола уз Конвенцију о високотехнолошком криминалу који се односи на инкриминацију дела расистичке и ксенофобичне природе извршених*

преко рачунарских система, Службени гласник Републике Србије број 19/09.
6. *Закон о одговорности правних лица за кривична дела*, Службени гласник Републике Србије, број 97/08.
7. Jagatic, T., Johnson, N., Jakobsson, M., Menczer, F. (2005). *Social Phishing*, School of Informatics, Indiana University, http://markus-jakobsson.com/papers/jakobsson-commacm07.pdf, доступан 15. 1. 2013.
8. Janczewski, L., Colarik, A. (2008). *Cyber Warfare and Cyber Terrorism*. Hershey, New York.
9. Knowem (2019). https://knowem.com, доступан 15. 5. 2019.
10. *Кривични закон Републике Србије*, Службени гласник СРС, бр. 26/77, 28/77, 43/77, 20/79, 24/84, 39/86, 51/87, 6/89 и 42/89, Службеник гласник РС, бр. 21/90, 16/90, 26/91, 75/91, 9/92, 49/92, 51/92, 23/93, 67/93, 47/94, 17/95, 44/98, 10/02, 11/02, 80/02, 39/03 и 67/03.
11. *Кривични законик Републике Србије*, Службени гласник РС бр. 85/2005, 88/2005 – испр., 107/2005 – испр., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014 , 94/16, 35/19.
12. Мандић, Г., Путник, Н., Милошевић, М. (2017). *Заштита података и социјални инжењеринг – правни, организациони и безбедносни аспекти*. Универзитет у Београду Факултет безбедности, Београд.
13. Mathew, T. (2004). *Ethical Hacking and Countermeasures [EC-Council Exam 312-50] — Student Courseware.* OSB Publisher, International Council of Electronic Commerce Consultants, New York.
14. Милошевић, М. (2012). *Одговорност правних лица за кривична дела, докторска дисертација.* Правни факултет Универзитета у Београду, Београд.
15. Милошевић, М. (2012а). Кривична одговорност правних лица у англоамеричком праву. *Страни правни живот*, 56(2): 230–251.
16. Милошевић, М., Симовић, И. (2018). Појам одговорног лица у Закону о одговорности правних лица за кривична дела. У: *Кривично законодавство и функционисање правне државе, међународна научно-стручна конференција*, стр. 365–382. Требиње, 20. и 21. 04. 2018. године, Министарс-

тво правде Републике Српске, Српско удружење за кривичноправну теорију и праксу, Град Требиње.
17. Мирић, Ф. (2018). Интернет превара као облик компјутерског криминалитета. *Зборник радова Правног факултета у Нишу*, 57(80), 531–542.
18. Namechk (2019). https://namechk.com, доступан 15. 5. 2019.
19. Ollmann, G. (2004). *The Phishing Guide*, http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf, доступан 14. 1. 2013.
20. Phishing without borders, or why you need to update your router (2019)https://www.kaspersky.com/blog/hacked-routers-dns hijacking/26802/?utm_source=facebook&utm_medium=social&utm_campaign=rs_hacked-routers-dns hijacking_ma0111_organic&utm_content=sm-post&utm_term=rs_facebook_organic_ma0111_sm-post_social_hacked-routers-dns-hijacking, доступан 14. 5. 2019.
21. Pipl (2019). https://pipl.com/corp/blog, доступан 15. 5. 2019.
22. Путник, Н. (2009). *Сајбер простор и безбедносни изазови*. Факултет безбедности, Београд.
23. Путник, Н., Милошевић, М. (2016). Смернице за израду политике безбедности информационо-комуникационих ресурса и њихових корисника у образовно-васпитном систему". У зборнику (приредили: Бранислава Поповић Ћитић, Милан Липовац): *Безбедност у образовно-васпитним установама: основна начела, принципи, протоколи, процедуре и* средства. стр. 97–116. Факултет безбедности, Београд.
24. Rittinghouse, J., Hancock, W. (2003). *Cybersecurity Operations Handbook*. Elsevier, Burlington.
25. Shinder, D. L. (2002). *Scene of the Cybercrime: Computer Forensics Handbook*. Syngress Publishing, Inc., Rockland.
26. Skoudis, E. (2002). Counter *Hack: A Step-By-Step Guide to Computer Attacks and Effective Defenses*. Prentice Hall, New Jersey.
27. Стојановић, З. (2012). *Коментар Кривичног законика*. Службени гласник, Београд.

28. Стојановић, З., Делић, Н. (2015). *Кривично право – посебни део*, Правна књига, Краљево.
29. Findface (2019). https://findface.ru, доступан 19. 5. 2019.
30. How cybercriminals harvest information for spear phishing (2019). https://www.kaspersky.com/blog/spearphishers-information/25589, доступан 18. 5. 2019.
31. Šta je DNS i koji je najbrži DNS? (2018). https://balkanandroid.com/sta-je-dns-i-koji-je-najbrzi-dns, доступан 14. 5. 2019.

The specific features of perpetration of the criminal offence of fraud using information-communication technologies

Abstract: *Historically speaking, along with the development of ICT, the ways of their misuse developed as well. Whoever may have bad intentions will keep finding new methods to abuse these technologies. These methods are based on vulnerabilities of ICT systems, whether they are technical or related to human factor.*

This paper describes the phenomena of the so-called social engineering and phishing, as modes of performing the criminal offences of fraud and computer fraud, which are used for illegal collection and abuse of the data of ICT system users, in order to mislead them towards acting in a way that causes harm to their own or someone else's possession, with the intention of illegal gain for the perpetrator. Contemporary phishing attacks are very sophisticated, adapted to the potential victims and adjusted to their affinities. The collecting of information regarding a potential victim is most often done via social networks. Therefore, this paper describes the process of planning acts of fraud and explains two most common techniques for data collecting – via social networks and via the victim's illegal router hijacking.

A special emphasis is put on the criminal law treatment of these phenomena in the legislation of the Republic of Serbia, as well as on solving the dilemmas about technical terms in fraudulent acts in Serbian and English languages. The authors present different forms of social engineering and phishing in ICT systems, i.e. cyberspace, and

discuss if and in which cases their acts have legal characteristics of the aforementioned criminal offences.
The authors also present and analyze Serbian criminal legislation,with the emphasis on the crime of fraud and similar crimes, which are, in their essence, special forms of fraud. The stress is put on the crime of computer fraud and its characteristic features in comparison with the crime of fraud. The authors consider the changes in legislation that would lead to reformulating the crime of computer fraud so as to encompass various acts carried out with the use of the information-communication technologies.

Key words: *High-tech crime, criminal act of fraud, criminal act of computer fraud, social engineering, phishing, cyberspace.*