Др *Владимир УРОШЕВИЋ*,
МУП Републике Србије

„Нигеријска превара“ у Републици Србији

УДК: 343.522 : 004.738.5(497.11)

Апстракт: *Један од најраспрострањенијих облика кривичних дела преваре који се врши уз помоћ рачунара је превара позната као „нигеријска превара“ или „Превара 419“. „Нигеријска превара“ представља специфичан начин извршења кривичног дела преваре који је настао захваљујући глобалној улози интернета као средства за комуникацију, електронско пословање и сл., као и све већој употреби савремених информационих технологија од стране великог броја крајњих корисника, широм света. Први појавни облици ове преваре подразумевали су лажне пословне понуде које су извршиоци кривичних дела нудили жртвама преваре. Данас начини извршења ових облика превара имају различиту форму, па се тако врше помоћу лажних електронских порука о добицима на играма на срећу, лажних порука везаних за добротворне прилоге, порука у вези са „љубавним понудама“ и др. Развој савремених информационих технологија пружа све више техничких могућности за вршење овог облика преваре, а жртве су појединци и предузећа широм света. Грађани Републике Србије и предузећа са наше територије такође су угрожени тим видом преваре. У овом раду објашњен је појам „нигеријске преваре“, приказани су начини њеног извршења, правна регулатива у Републици Србији везана за спречавање ове појаве, као и досадашња искуства МУП-а Републике Србије у вези спречавања „нигеријских превара“ у Републици Србији.*

Кључне речи: *превара, рачунарска превара, нигеријска превара, високотехнолошки криминал, информационе технологије.*

Увод

Појава интернета, као и све већа, глобално распрострањена употреба информационих и телекомуникационих технологија, утицала је на пораст илегалних активности у овом простору. Употреба рачунарских сервера који пружају опције анонимног коришћења интернета, могућност отварања Web електронске поште и коришћења лажних електронских адреса, постављање лажних интернет сајтова и др., данас су основно оруђе у рукама извршилаца кривичних дела превара које се врше помоћу савремених информационих технологија.

„Преваре 419“ као облик кривичних дела превара које се врше уз помоћ рачунара данас су постале веома честа и распрострањена појава, која је од стране многих полицијских служби широм света означена као веома велика опасност по финансијску безбедност, како појединаца, тако и држава. Од стране многих организација као најризичније државе из којих се врше ове врсте превара означене су државе Западне Африке: Нигерија, Гана, Бенин, Обала Слоноваче, Того и Буркина Фасо. Ван територије Западне Африке, као најризичније државе са чијих се територија врше те врсте превара означене су Јужна Африка, Шпанија и Холандија.[1]

Као веома специфичан облик преваре који има међународне размере и изазива оштећења која се могу исказати стотинама милиона америчких долара, „нигеријска превара“ заслужује посебну пажњу и посебну анализу.

Грађани Републике Србије који су корисници интренета, као и државне институције, јавне установе и предузећа са наше територије у којима се користи интернет у пословању, изложени су ризику који је настао као последица деловања тих криминалних група.

Појам „нигеријске преваре“

„Нигеријска превара“, или превара позната под називом „превара 419“, појавила се раних 80-тих година, са наглим економским развојем Републике Нигерије, који се заснивао на употреби нафтних ресурса. Неколико незапослених студената са нигеријског универзитета почело је у раним 80-тим и средином 90-тих да употребљава методе те преваре како би довели у заблуду пословне људе са Запада који су били заинтересовани за „тајанствене“ послове у нигеријском нафтном сектору, а касније су те методе почели да употребљавају и на широј популацији. У току прве деценије 21-ог века „превара 419“ постала је веома популаран начин извршења кривичних дела преваре у Африци, Азији и Источној Европи, а у последње време и у Северној Америци, Западној Европи (углавном Великој Британији) и Аустралији.

„Превара 419“, као израз за „нигеријску превару“, добила је назив по члану број 419 *Нигеријског кривичног закона* (који је део поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“, који дефинише ово кривично дело (Chawki, 2009:2). Америчко друштво за дијалектику је утврдило да се израз „превара 419“ користи од 1992. године.

„Нигеријска превара“ је метода вршења кривичног дела преваре уз помоћ рачунара и најчешће почиње писмом или електронском поруком која је тако осмишљена да изгледа као да је намерно послата примаоцу поруке. Радња извршења „нигеријске преваре“ углавном почиње убеђивањем „жртве“ преваре да учествује у подели одређених новчаних фондова ако

[1] http://en.wikipedia.org/wiki/Advance-fee_fraud, дана 14.11.2009. године.

унапред уплати одређени новчани износ који је, у највећем броју случајева, неупоредиво мањи од оног износа који би требало да добије као корист од тог фонда (Smith et al., 1999:1).

Електронском поруком (најчешће SPAM поруком) од примаоца поруке се тражи помоћ за трансфер великих новчаних износа, за који ће након обављеног трансфера добити одређени проценат као надокнаду. У таквим порукама се нпр. наводи да је:

- реч о великој суми новца која је позната само пошиљаоцу поруке, и да он чека да буде исплаћена као резултат одређених банкарских малверзација и сл.;
- пошиљалац поруке члан нигеријске владе или нигеријске војске и покушава да изнесе већу количину новца из Нигерије, али да му је за то потребна помоћ из иностранства;
- пошиљалац поруке спреман да новац подели са оним ко му помогне да изврши трансфер одређене суме новца (нпр. прање новца);
- тајност посла апсолутна потреба, пошто би корумпирани званичници Нигерије присвојили новац за себе уколико би сазнали да он постоји (Buchanan et al., 2001:40).

Начин извршења „нигеријске преваре“

Извршиоци кривичног дела преваре шаљу електронске поруке корисницима интернета, са намером да понуде неки примамљив посао у нади да ће жртва преваре на крају уплатити одређени износ новца на име његове реализације (нпр. разне измишљене надокнаде за ангажовање стручних лица или адвокате, за издавање потребних дозвола за реализацију посла, уплате административних такси и друго). Те електронске поруке насловљена су генерално на било ког примаоца поруке, и из њих се не може видети коме се пошиљалац обраћа, а њихов контекст је такав да прималац поруке лако може помислити да се порука односи управо на њега. Уколико жртва преваре одговори на прву поруку, она се методом социјалног инжењеринга наводи да помисли да је њена помоћ неопходна да би се одређена радња извршила (нпр. трансфер новца, уручивање наследства и др.).[2] Детаљи у порукама могу да се разликују, али садржина самог писма које стиже жртвама преваре најчешће се односи на то да особа која је наводни пошиљалац поруке није у могућности да сама изврши одређене радње, те да јој је зато потребна помоћ примаоца поруке. Особе које се наводе у тим порукама

[2] Социјални инжињеринг је акт манипулације којим се људи наводе да одају поверљиве информације о себи. Та техника заснива се на ометању пажње одређеног лица у циљу прикупљања информација које оно иначе не би одало, а како би се ти подаци касније злоупотребили (ради одавања корисничких имена, лозинки или, нпр. података о платним картицама). Све методе социјалног инжињеринга заснивају се на специфичним правилностима у процесу доношења одлука, познатијем као „погрешна когниција“, која представља образац неправилног просуђивања људи који се појављују у одређеним, специфичним ситуацијама.

најчешће стварно постоје, али су њихови идентитети украдени без њиховог знања и користе се од стране извршилаца кривичних дела како би се прикрио њихов прави идентитет, или како би се снагом ауторитета одређених лица улило поверење жртвама преваре и придобило њихово поверење.

У тим порукама помињу се суме новца које се крећу и до неколико милијарди америчких долара, затим злато, „прљав" новац на банковним рачунима, „крвави дијаманати", серије чекова и др. Суме новца укључују милионе долара које ће наводни инвеститори на крају посла поделити са жртвом преваре, а проценат зараде који се обећава креће се и до 40 % од суме новца која је предмет „посла".

Оштећена лица се методама социјалног инжињеринга при комуникацији наводе да уплате један мали проценат од укупне суме новца која је предмет „посла". Уплату тих новчаних износа извршиоци кривичних дела траже како би се нпр. надокнадили одређени трошкови које сноси неко измишљено лице (нпр. трошкови подмићивања, накнаде у банкама, трошкови адвоката и др.) да би дошли до предметног новца.

Највећи број извршилаца ових кривичних дела припада мањим организованим криминалним групама, али се понекад дешава да функционишу и самостално. Уколико извршиоци кривичних дела нису добро организовани, онда не могу да изврше преваре већих размера и оштете веће компаније, али су јако опасни за средњу класу грађана и мала предузећа.

Ако жртва преваре пристане на понуђени „посао", извршиоци кривичних дела јој шаљу један или више фалсификованих докумената са лажним печатима, потписима, лажном садржином и сл. Извршиоци који врше ове преваре често користе лажне податке и крађу идентитета, те тако врло често при представљању користе фотографије других лица које су прикупили са интернета како би се лажно представили оштећенима.

Након што оштећени уплати одређени новчани износ према инструкцијама извршилаца кривичних дела следи одлагање новчаних трансакција везаних за исплату обећане суме новца. Стално се појављују нови трошкови за оштећеног на име реализације посла и траже нова одлагања, стално се обећава „експресна" исплата новца, уз убеђивање жртве преваре да ће јој се улагање у договорени посао вишеструко исплатити.

Психолошки притисак се на жртве преваре додатно врши и навођењем да је тајност „посла" јако потребна, пошто би корумпирани званичници неке државе присвојили новац за себе уколико би сазнали да он постоји (Buchanan et al., 2001:40). Такав притисак понекад жртва преваре додатно врши и сама над собом (нпр. када и након што сазнају да су преварене, жртве преваре наставе комуникацију да би повратиле новац, пронашле извршиоце и сл.).

Извршиоци кривичних дела се ослањају на чињеницу да ће за време које прође док жртва схвати да је преварена (тј. док схвати да обећани новац не постоји), новчани трансфер који је она извршила на њихове рачуне

бити исплаћен, те да оштећени неће стићи на време да блокира трансфер. Од оштећених се најчешће тражи да новац уплате преко Western Union-a и MoneyGram-a због брзине преноса новчаних средстава и анонимности примаоца уплате, чиме се смањује могућност откривања извршилаца.

Електронске поруке, као што су SPAM-ови са оваквом садржином, најчешће се шаљу из интернет кафеа. У Нигерији, у областима као што су нпр. Лагос или Фестак, постоје многи интернет кафеи који су отворени управо у те сврхе, а радно време им је од 22,30 часова до 07,00 часова, ради избегавања контроле од стране државних службеника. Чињеница је да извршиоци ових кривичних дела користе информационе технологије да би сакрили свој идентитет и физичку локацију, како би осујетили напоре полицијских служби да их открију (Chawki, 2006:5). Поред тога што успоравају рад рачунара корисника на интернету, ове поруке подижу и цену коришћења употребе интернета крајњим корисницима пошто интернет сервис провајдери морају додатно да улажу у своју опрему како би их заштитили од нежељене електронске поште овог типа (Longe et al., 2008:138).

У многим државама постоје и предузећа која уз новчану надокнаду обезбеђују лажна документа која се користе у овим преварама.[3] Са жртвама кривичних дела извршиоци комуницирају и преко мобилних телефона, користећи припејд SIM картице, које лако могу да баце и потом купе нове ради даље комуникације.

Како би извршили кривично дело преваре овог типа, извршиоци најчешће користе фалсификовану документацију како би преузели новац који им је оштећени уплатио, бежичне трансфере новца за пренос противправно стечених новчаних средстава, техничка средства која им омогућују анонимну комуникацију, Web-базирану електронску пошту, електронске налоге који су предходно преузети од правих корисника, факс машине за слање факс порука при размени документације са жртвама преваре, услуге телекомуникационих сервиса за директну комуникацију са жртвом преваре, постављају лажне странице на интернету којима оштећене доводе у заблуду да комуницирају и сарађују са представницима легалних и легитимних институција, уговарају пословне састанке са оштећенима (приликом комуникације извршиоци кривичних дела обећавају специјалне аранжмане, као што је нпр. улазак у Нигерију без визе и слично, након чега се жртве ових кривичних дела које дођу у контакт са извршиоцима киднапују, захтева се откуп и сл. (Dyrud, 2005:4).

---

[3] Након једне преваре која је укључивала лажни потпис нигеријског председника Olusegun Obasanjo у лето 2005. године, нигеријске власти извршиле су претресе на тржници у делу Лагоса под називом Oluwole. Заплењене су хиљаде нигеријских и других пасоша, 10.000 бланко British Airways карата, 10.000 налога за исплату новца из САД, царинска документација, лажна уверења универзитета, 500 компјутера са скенираном документацијом који су служили за прављење фаслификоване документације и др.
Извор:http://web.archive.org/web/20051029165224/http://news.yahoo.com/s/latimests/20051020/ts_latimes/iwilleatyourdollars, дана 07.09.2009. године.

Законски и институционални оквири за спречавање „нигеријских превара“ у Републици Србији

У *Кривичном законику*, који је ступио на снагу 1. јануара 2006. године, објављеном у Службеним гласницима Републике Србије, број 85/2005, 88/2005 и 107/2005, у поглављу XXI под називом „Кривична дела против имовине“, у ставу 1 члана 208, кривично дело Превара се дефинише на следећи начин:

„Ко у намери да себи или другом прибави противправну имовинску корист доведе кога лажним приказивањем или прикривањем чињеница у заблуду или га одржава у заблуди и тиме га наведе да овај на штету своје или туђе имовине нешто учини или не учини, казниће се новчаном казном или затвором до три године“.

У ставу 2 се наводи да ће се учинилац овог кривичног дела казнити новчаном казном или затвором до шест месеци ако дело учини само у намери да другог оштети. У ставу 3 се наводи да ће се затвором од једне до осам година учинилац казнити ако је делом из става 1 и става 2 прибављена имовинска корист или је нанета штета у износу који прелази 450.000,00 динара. У ставу 4 наведено је да ће се казном од две до десет година учинилац казнити ако је делом из става 1 и 2 прибављена имовинска корист или је нанета штета која прелази 1.500.000,00 динара.

Новим *Законом о изменама и допунама кривичног законика* од 31.08.2009. године, који је објављен у Службеном гласнику Републике Србије, број 72-09, а који је ступио на снагу дана 08.09.2009. године, чланом број 68 предвиђене су измене у члану 208, где су у ставу 1 речи: „новчаном казном или затвором до три године“ замењене речима: „затвором од шест месеци до пет година и новчаном казном“ У ставу 2 речи: „новчаном казном или затвором до шест месеци“ замењене су речима: „затвором до шест месеци и новчаном казном“. У ставу 3, после речи: „осам година“, додате су речи: „и новчаном казном“, а у ставу 4 после речи: „десет година“, додате су речи: „и новчаном казном“.

У члану 2 је предвиђено да ће се затвором до шест месеци и новчаном казном казнити ко дело из става 1 овог члана учини само у намери да другог оштети, чланом 3 се предвиђа да ће се учинилац казнити затвором од једне до осам година и новчаном казном ако је делом из ст. 1 и 2 овог члана прибављена имовинска корист или је нанета штета у износу који прелази 450.000 динара. У ставу 4 је предвиђено да ће се учинилац казнити затвором од две до десет година и новчаном казном ако је делом из ст. 1 и 2 тог члана прибављена имовинска корист или је нанета штета у износу који прелази 1.500.000 динара.

У *Кривичном законику* који је ступио на снагу 1. јануара 2006. године, у поглављу XXVII под називом „Кривична дела против безбедности рачу-

нарских података“, у ставу 1 члана 301, такође се дефинише и радња извршења кривичног дела Рачунарска превара, и то на следећи начин:

„Ко унесе нетачан податак, пропусти уношење тачног податка или на други начин прикрије или лажно прикаже податак и тиме утиче на резултат електронске обраде и преноса података у намери да себи или другом прибави противправну имовинску корист и тиме другом проузрокује имовинску штету, казниће се новчаном казном или затвором до три године.“ У ставу 2 овог члана се наводи да ће се учинилац казнити затвором од једне до осам година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 450.000 динара. Ставом 3 је предвиђено да ће се учинилац казнити казном затвора од две до десет година ако је делом из става 1 тог члана прибављена имовинска корист која прелази износ од 1.500.000 динара. Чланом 4 предвиђена је новчана казна или затвор до шест месеци уколико је дело из става 1 тог члана извршено само у намери да другог оштети.

Новим *Законом о изменама и допунама кривичног законика*, који је ступио на снагу дана 08.09.2009. године, у члану 119 тог *Закона* предвиђен је и члан 304а, који гласи: „Прављење, набављање и давање другом средстава за извршење кривичних дела против безбедности рачунарских података“. У ставу 1 овог члана начин извршења овог кривичног дела дефинисан је на следећи начин: „Ко поседује, прави, набавља, продаје или даје другом на употребу рачунаре, рачунарске системе, рачунарске податке и програме ради извршења кривичног дела из чл. 298 до 303 тог *Законика* казниће се затвором од шест месеци до три године“. У ставу 2 предвиђено је да ће се предмети из става 1 овог члана одузети.

На описани начин законодавац је омогућио кривично правну заштиту лица и имовине и створио правне оквире за ефикасно спречавање кривичних дела рачунарске преваре.

Институционални оквир за борбу против ових кривичних дела, постављен је у *Закону о организацији и надлежности државних органа за борбу против високотехнолошког криминала*, који је објављен 15.07.2005. године у Службеном гласнику Републике Србије, број 61/05. Овим Законом уређује се образовање, организација, надлежност и овлашћења посебних организационих јединица државних органа ради откривања, кривичног гоњења и суђења за кривична дела одређена тим *Законом*. У члану 2 се, између осталог, наводи да високотехнолошки криминал у смислу тог *Закона* представља вршење кривичних дела код којих се као објекат или средство извршења кривичних дела јављају рачунари, рачунарске мреже, рачунарски подаци, као и њихови производи у материјалном или електронском облику, а под производима у електронском облику посебно се подразумевају рачунарски програми и ауторска дела која се могу употребити у електронском облику. У члану 3, у ставу 1 је наведено да се тај *Закон* примењује ради

откривања, кривичног гоњења и суђења за кривична дела против безбедности рачунарских података одређена кривичним законом.

Наведеним *Законом* су установљене институције за борбу против високотехнолошког криминала: Посебан тужилац за високотехнолошки криминал Окружног јавног тужилаштва у Београду надлежан за читаву територију Републике Србије, Савет за борбу против високотехнолошког криминала Окружног суда у Београду и Служба за борбу против високотехнолошког криминала у оквиру МУП-а Републике Србије.[4]

Дана 18.03.2009. године у Службеном гласнику Републике Србије, број19-09 објављен је и *Закон о потврђивању Конвенције о високотехнолошком криминалу*. У члану 3 тог *Закона* наводи се да су за њено спровођење задужени министарство надлежно за правосуђе, министарство надлежно за унутрашње послове и министарство надлежно за телекомуникације.

На описани начин на територији Републике Србије створени су кривично-правни и институционални оквири за борбу против високотехнолошког криминала, а тиме и за борбу против кривичних дела преваре и рачунарских превара на интернету.

Искуства у спречавању „нигеријских превара“ на територији Републике Србије

У току 2008. и 2009. године на територији Републике Србије од стране оштећених лица пријављено је девет кривичних дела преваре са елементима „нигеријских превара“ против непознатих учинилаца. Овим кривичним делима оштећени су држављани Републике Србије и предузећа са наше територије, а укупна имовинска штета износила је преко 60.000 ЕУР-а. Оштећена лица су новац извршиоцима кривичних дела слали преко сервиса Western Union и MoneyGram. Преваре су углавном вршене помоћу SPAM порука уз коришћење методе социјалног инжињеринга, а комуникација је, након одговора од стране оштећених на SPAM поруку, углавном вршена преко бесплатних налога за електронску пошту која је отварана на интернет сервисима Yahoo, Hotmail и др. Такође су употребљаване и лажне интернет адресе на којима су се налазиле интернет презентације постављене од стране извршилаца кривичних дела са намером да обману оштећене. Употребљавана је и фалсификована документација државних органа и предузећа Нигерије, Гане и других држава са територије Западне Африке.

Извршиоци кривичних дела „нигеријске преваре“ углавном су ова дела вршили слањем нежељених, тзв. SPAM порука. За скривање идентитета на интернету извршиоци су користили приступе на јавним местима, као нпр. у cyber кафеима, пошто се посетиоци ових сервиса често идентифи-

[4] У МУП-у Републике Србије, у оквиру Службе за борбу против организованог криминала, основано је Одељење за борбу против високотехнолошког криминала.

кују јединственом ознаком која представља само генерални идентификатор одређеног компјутера или места конекције. У комуникацији са оштећеним лицима са наше територије коришћени су идентитети званичника наведних држава, свештеника, адвоката и сл.

Коришћење интернет сервиса и програма на интернету, за прикривање IP адреса такође је веома распрострањено. Ти сервиси извршоцима омогућују анонимно слање електронских порука, без остављања трага о правој IP адреси извршиоца кривичног дела, на тај начин што целокупан интернет саобраћај према одређеним интернет адресама и страницама иде преко сервиса који потом као траг оставља своју IP адресу, а адреса правог корисника се налази на серверу ових сервиса.

Прикривање идентитета врши се на много различитих начина, а већина случајева прикривања везана је за сакривање идентитета лица које је осмислило превару и лица које злоупотребљава податке о жртвама преваре.

Пошто се ради о простору где се време реакције мора сводити на секунде, кључна је брза и ефикасна реакција. Шанса за проналазак доказа у оваквом окружењу зависи од саме конфигурације умрежених рачунара који се појављују у комуникацији као рачунарски сервери, улазне капије, рутери и др. Лог фајлови су главни извор проналаска трагова и доказа о извршеном кривичном делу.

Прве информације о илегалној активности најчешће не воде до правог идентитета лица, већ се прикупљају подаци са више локација, често и широм света, преко Интерпола. На међународном нивоу у полицијској и правосудној сарадњи још није постигнут довољно добар квалитет сарадње потребан за такве врсте истрага.

Након сазнања да је извршена та врста преваре и да је дошло до злоупотребе података који су од стране извршилаца кривичних дела прикупљени на напред описане начине, полицијски службеници прикупљају доказе и трагове у виду електронских података о остваренoj комуникацији која се одвијала између извршилаца кривичних дела и оштећених, као и податке о финансијским трансакцијама које је оштећени извршио према инструкцијама које је добио од извршилаца. Врше се провере лог фајлова у потрази за IP адресом, како би се лоцирао сервис преко кога је извршилац кривичног дела слао електронске поруке оштећеном, као и преглед целокупне електронске поште коју је оштећени примио, како би се уочили пропусти направљени од стране извршиоца који могу указати на постојање кривичног дела (нпр. у случају да је извршилац поставио лажни интернет линк неке институције, провером места хостовања правог интернет сајта институције и лажног сајта може се уочити да се ради о превари) и места одакле је извршена превара. Након изоловања IP адресе и времена слања електронских порука из лог фајлова, преко Интерпола се, у зависности од државе са чије је територије извршено кривично дело, врше провере у вези са корисником

коме је она била додељена у тренутку вршења кривичног дела.

Како би се детекција електронских порука свела на што мањи ниво, извршиоци кривичних дела данас шаљу мање количине SPAM порука са рачунара заражених рачунарским вирусима, како би се обезбедило што дуже функционисање њиховог слања. Неки комерцијални SPAM сервиси укључују botnet мреже за слање ових порука, које помажу да се избегну анти - SPAM мере на рачунарима корисника и заштите на серверима интернет провајдера, које функционишу на тај начин што се блокирају IP адресе које су постављене на „црне листе“. Данас постоји велики број IP адреса са којих је вршено слање ових порука и које су идентификоване као носиоци SPAM активности. „Црне листе“ се врло често ажурирају, па извршиоци кривичних дела који користе слање оваквих порука за прибављање података морају да ангажују botnet мреже како би избегли блокирање њиховог пријема. Такав начин слања SPAM порука додатно отежава рад полицијских служби МУП-а Републике Србије, пошто корисници интернета на територији Републике Србије и не сумњају да поруке које им стижу могу бити штетне. Из наведеног разлога сматра се да постоји и велика „тамна бројка“ када су „нигеријске преваре“ у питању пошто оштећена лица или нису свесна да су преварена, или их је због околине срамота да пријаве да су оштећени. Оштећени се често плаше да пријаве такве случајеве пошто их извршиоци кривичних дела убеђују да су сами криви за то што посао није могао да се реализује, прете им да ће их тужити и сл.

У случајевима „нигеријских превара“ чије су жртве држављани Републике Србије радило се о преварама извршеним на неколико начина, и то: слањем обавештења о лажним добицима на лутрији помоћу којих су жртве превара методама социјалног инжињеринга навођене да поверују да су добитници награда, након чега су уплаћивали одређене суме новца да би им се омогућило подизање награде, и слањем обавештења о наследству помоћу којих су жртве превара методама социјалног инжињеринга навођене да поверују да су наследиле одређену количину новца, након чега су уплаћивали одређене суме новца да би им се омогућила исплата наслеђеног новца. Кривична дела су иницирана са подручја Нигерије, Сенегала и Бенина, а међународна полицијска сарадња са наведеним државама до данас није довела до значајнијих резултата.

Закључак

Интернет је још увек правно нерегулисан простор, у коме извршиоци кривичних дела имају доста простора за вршење криминалних активности. Развој савремених информационих технологија, посебно на пољу електронске трговине и комуникације, створио је нови простор за деловање криминалаца и криминалних група. „Нигеријске преваре“ су, из наведених

разлога, постале један од најчешћих облика превара на интернету, због врло честог мењања начина извршења и прилагођавања брзим променама у области информационих технологија.

Наведена појава се може ефикасно спречавати једино акцијама на глобалном нивоу, како би се створила свест о опасности коју она са собом носи. Потребно је да се предузму активности на расветљавању начина извршења тих кривичних дела и њиховог презентовања широј јавности путем јавних гласила (новине, телевизија), а такође је потребно појачати и сарадњу на националном, регионалном и глобалном плану, посебно када су у питању међународна полицијска и кривичноправна сарадња.

Правна регулатива у Републици Србији пружа добру основу за ефикасно спречавање овог вида кривичног дела преваре. Међутим, као основни проблем јавља се чињеница да се ова кривична дела врше од стране лица која се налазе ван територије Републике Србије, углавном са територије афричког континента, са којима је међународна полицијска сарадња знатно отежана.

Чињеница је да феномен „нигеријских превара“ код нас није довољно познат широј јавности и корисницима интернета, посебно зато што та тема није довољно заступљена у медијима. Превентивно деловање државних органа као што су полиција и тужилаштво има кључну улогу када је спречавање те појаве у питању. Пошто сарадња са државама из којих се врши ова врста кривичних дела није на завидном нивоу, потребно је што хитније деловати проактивно, искористити потенцијал медија и скренути пажњу домаћој јавности на финансијске губитке који настају као последица тих кривичних дела. Превентивна улога полиције у заштити корисника интернета са територије Републике Србије од „нигеријских превара“ таквим активностима сигурно би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично дело извршено.

Литература:

1. Buchanan, J., Grant, A., (2001), *Investigating and Prosecuting Nigerian Fraud*, U.S. Attorneys' Bulletin, Vol 49, No 06, USA, стр. 39-47.
2. Chawki, M., (2006), *Anonymity in Cyberspace: Finding the Balance between Privacy and Security*, Revista da Faculdade de Direito Milton Campos, Nova Lima, Brazil, vol 11, стр. 39-64.
3. Chawki, M., (2009), *Nigeria Tackles Advance Fee Fraud*, Journal of Information, Law & Technology, University of Warwick, Great Britain, (1), сстр. 1-20.

4. Dyrud, M., (2005), *I brought You a good news An analysis of Nigerian 419 Letters*, Proceedings of 2005 Annual Association for Business Communication, Convention Association for Business Communication, USA, стр. 11.
5. Longe, B., Chiemeke, C., (2008), *Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing?*, European Journal of Social Sciences – Volume 6, Number 4, Great Britain, стр. 132-139.
6. Smith, R., Holmes, M., Kaufmann, P., (1999), *Nigerian Advance Fee Fraud*, Trends and Issues in crime and criminal justice, Australian Institute of Criminology, Australia, стр. 1.

'Nigerian Fraud' in the Republic of Serbia

Abstract: *One of the most widespread forms of cyber fraud is a fraud known as "Nigerian fraud" or "419 Fraud". The "Nigerian fraud" is a special form of fraud which is caused by global use of the Internet as a means of communication, electronic business etc., as well as the increased use of modern information technology by users throughout the world. First forms of this fraud were presented as false business proposals made by criminals and offered to victims of fraud. Today ways of conducting this type of fraud have different forms and can be done as lottery scams, charity scams, "love scheme" scams, etc. Development of modern information technology provides lots of technical possibilities for performing this type of fraud. The victims are individuals as well as companies throughout the world. Citizens of the Republic of Serbia and companies on our territory are also threatened by this form of fraud. This article explains what Nigerian fraud is and in what ways it can be performed. The paper also explains legal provisions of The Republic of Serbia concerning prevention of this criminal act as well as experiences of the Ministry of the Interior of the Republic of Serbia regarding prevention of "Nigerian fraud".*

Key Words: *fraud, computer fraud, Nigerian fraud, high-tech crime, information technologies*