***Др Филип Мирић,****
*Самостални стручно-технички сарадник*
*Правног факултета,*
*Универзитет у Нишу*

ПРЕГЛЕДНИ НАУЧНИ РАД
doi:10.5937/zrpfni1880531M

*UDK: 004.738.5:343.3/.7*
*Рад примљен: 30.09.2018.*
*Рад прихваћен: 23.10.2018.*

# *ИНТЕРНЕТ ПРЕВАРА КАО ОБЛИК КОМПЈУТЕРСКОГ КРИМИНАЛИТЕТА***

***Апстракт*****:** *Развој интернета је довео до лакшег и бржег преноса информација и њихове веће доступности. Нажалост, пораст броја корисника интернета и његових сервиса створио је услове за вршење најразличитијих кривичних дела. Од свих противправних дела против имовине извршених на интернету највише пажње јавности привлаче преваре. У раду су изложене основне кривичноправне и криминолошке карактеристике интернет преваре као облика компјутерског криминалитета. Посебно су истакнуте разлике и сличности између рачунарске преваре и класичног кривичног дела преваре у кривичном законодавству Републике Србије. Дати су и начелни предлози за унапређење кривичноправне заштите корисника интернета. Анализиран је и настанак и механизам деловања такозване „нигеријске преваре", чије су жртве биле и многи грађани Србије. Коначно, аутор је у раду указао и на значај примарне превенције за сузбијање интернет превара уз навођење практичних савета за спречавање виктимизације у овој области, а са циљем да се на тај начин утиче на смањење распрострањености компјутерског криминалитета.*

***Кључне речи*****:** *кривично законодавство, имовински криминалитет, превара, компјутерски криминалитет, превенција.*

* filip@prafak.ni.ac.rs

** Рад је саопштен на међународној научној конференцији „Право пред изазовима савременог доба", која је одржана 13. и 14. априла 2018. године на Правном факултету Универзитета у Нишу.

## 1. Уводна разматрања

Развој компјутера и његових компоненти, као и константан пад њихових цена, довели су до тога да су компјутери данас доступни не само владама најмоћнијих држава у свету, већ да се они налазе у скоро сваком дому. Данас није потребно посебно знање за употребу компјутера, јер је начин њиховог коришћења сведен на ниво просечног човека. На тај начин повећан је и број потенцијалних делинквената у области компјутерских технологија (Димовски, 2010: 196). Појава великих технологија у индустрији компјутера и телекомуникација довела је до развоја нових врста криминалитета и створила нове технике за вршење традиционалних кривичних дела као што су превара и проневера (Константиновић Вилић, Николић Ристановић и Костић, 2012: 178). Рачунарски криминалитет је веома комплексан облик криминалитета. То је нова, савремена форма испољавања вршења кривичних дела која поприма интернационални карактер управо захваљујући савременом техничком и технолошком развоју (Јовашевић, 2006: 213). Криминалитет који се реализује помоћу компјутера може да има облик било ког од традиционалних видова криминалитета, као што су крађе, утаје, проневере, док се подаци који се неовлашћено прибављају злоупотребом информационих система, могу на различите начине користити за стицање противправне користи. У односу на штету или противправну корист коју овај вид криминалитета може да нанесе друштву или до које може да доведе, материјални и људски ресурси који се улажу су минимални, време извршења је веома кратко што додатно отежава откривање и доказивање дела, а веома често извршилац се уопште физички не налази на месту извршења дела (Вилић, 2016: 101). На само „клик" од нас су сада бројне информације које су пре само двадесетак година биле недоступне или тешко доступне. И поред свих предности глобалне светске рачунарске мреже (World wide web – WWW), на њој вребају и бројне опасности, које у мањој или већој мери угрожавају безбедност и сигурност њених корисника (Мирић, 2017: 56). Веома озбиљну претњу по безбедност корисника интернета представља рачунарска и интернет превара, о чему ће бити више речи у редовима који следе.

## 2. Рачунарска и интернет превара у кривичном законодавству Републике Србије и судској пракси

Живот је далеко испред могућности законодавца да инкриминише све потенцијално опасне друштвене појаве које су у вези са савременим технологијама. Број кривичних дела која се могу подвести чак и под

најрестриктивније и најуже дефиниције сајбер криминала (cybercrime), готово се свакодневно увећава (Комлен Николић et al., 2010: 13). Рачунарска превара је само једна од њих. Да би се она сагледала у кривичноправном смислу, неопходно је најпре, у најкраћем, указати на разлике и сличности између кривичног дела преваре и кривичног дела рачунарске преваре.

Превара и рачунарска превара су инкриминисана у кривичним законодавству Републике Србије.[1] Кривично дело преваре (чл. 208. КЗ) врши онај 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. Учинилац овог кривичног дела ће се казнити затвором од шест месеци до пет година и новчаном казном. Ко ово дело учини само у намери да другог оштети, казниће се затвором до шест месеци и новчаном казном. Овде је реч о привилегованом облику кривичног дела за који је предвиђено и блаже кажњавање у односу на основни облик. Ако је делом прибављена имовинска корист или је нанета штета у износу који прелази четристо педесет хиљада динара, учинилац ће се казнити затвором од једне до осам година и новчаном казном. Ако је делом прибављена имовинска корист или је нанета штета у износу који прелази милион и петсто хиљада динара, учинилац ће се казнити затвором од две до десет година и новчаном казном. У овом случају висина противправно стечене имовинске користи представља квалификаторну околност.

Са друге стране, кривично дело рачунарске преваре (чл. 301. КЗ) врши онај 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. За овакав преступ предвиђена је новчана казна или затвор до три године. Ово кривично дело има и један квалификован облик. Наиме, ако је извршењем овог кривичног дела прибављена имовинска корист у вишем износу од четристо педесет хиљада динара, учинилац ће се казнити затвором од једне до осам година. Ако је кривичним делом прибављена имовинска корист која прелази износ од милион и петсто хиљада динара, учинилац ће се казнити затвором од две до десет година. Ко наведено кривично дело учини само у намери да другог оштети, казниће се новчаном казном или затвором до шест месеци. И овде је реч о привилегованом облику кривичног дела у односу на основни облик кривичног дела. У односу на кривично дело рачунарске преваре, интернет

1 Кривични законик („Службени гласник РС“, бр. 85/2005... 94/2016, у даљем тексту: КЗ).

превара је уже одређена и представља злоупотребу софтвера са приступом интернету или мрежних сервиса, како би се остварила противправна имовинска корист или другом нанела штета.

Када је реч о сличностима кривичног дела преваре и рачунарске преваре, треба имати у виду да се и код једног и код другог кривичног дела радња извршења предузима у намери да учинилац оствари противправну имовинску корист. То је елемент бића овог кривичног дела. Последица је, дакле, иста код оба кривична дела. Извршилац може бити свако лице, а као облик, виности се захтева умишљај. Основна разлика између ова два кривична дела јесте у томе што се као средство извршења код кривичног дела рачунарске преваре јавља рачунар. Имајући то у виду, извршилац овог кривичног дела најчешће мора поседовати напредна знања и вештине из области информационих технологија. Управо ова специфичност је одлучујуће утицала на законодавца да кривично дело рачунарска превара инкриминише у глави посвећеној кривичним делима против безбедности рачунарских података, за разлику од преваре које представља типично имовинско кривично дело.

На овом месту корисно би било укратко указати на сличности разлике између рачунарске преваре и интернет преваре. Иако се за извршење и једног и другог кривичног дела користи рачунар, ипак између ових кривичних дела постоје и суштинске разлике. Превара путем интернета није увек и обавезно рачунарска превара, јер неке интернет преваре одговарају класичним преварама које за средство извршења имају интернет без неког посебног утицаја на електронску обраду података или рад рачунара (Вилић, 2016: 201). Једноставније речено, интернет преваром се обмањују људи, тј. корисници интернета, а рачунарском преваром се „обмањују" рачунари, односно системи за обраду података. Занимљиво је да интернет превара није инкриминисана као засебно кривично дело у кривичном законодавству Републике Србије. Имајући у виду штетност ове појаве, као и утицај интернета на животе људи, било би корисно размишљати о инкриминацији интернет преваре као засебног кривичног дела. Тиме би се кривичноправна заштита корисника интернета побољшала и значајно унапредила.

За свеобухватно сагледавање кривичних дела рачунарске преваре и интернет преваре од изузетног је значаја анализирати и релевантну судску праксу.[2] Нажалост, судска пракса је, када је реч о овом кривичном делу, веома скромна, па ће на овом месту бити приказан случај судске одлуке у коју је аутор овог рада имао увид.

2 У овом делу рада коришћене су сентенце релевантних судских одлука доступних у рачунарској бази правних прописа и судских одлука *Paragraf Lex.*

- Како је окривљени уношењем нетачних података на банкомату банке чији је комитент изиграо рачунарски систем и тиме себи прибавио знатну имовинску корист, одговоран је за кривично дело рачунарска превара.

Из образложења:

*„Из списа произилази да је ВЈТ у Б. поднело оптужни предлог Вишем суду у Б. против окривљеног због кривичног дела рачунарске преваре из члана 301. став 1. КЗ-а, међутим, првостепени суд је нашао да је за чињенични опис садржаног у оптужном предлогу ВЈТ-а у Б. произилазе елементи бића кривичног дела издавање чека и коришћење платне картице без покрића из члана 228, став 3 у вези са ставом 1 КЗ, будући да се окривљеном ставља на терет да је коришћењем платних картица за које није имао покриће прибавио себи имовинску корист у укупном износу од 1.282.882 динара, при чему је уношењем нетачних података утицао на резултате електронске обраде и преноса података, што је чинио како би прикрио чињеницу да у тренутку коришћења платне картице на рачуну нема покрића, те се у описима радњи не стичу објективна обележја кривичног дела рачунарске преваре из члана 301, став 1 КЗ-а већ кривичног дела издавања чека и коришћења платне картице без покрића из члана 228, став 3 у вези става 1 КЗ-а. Међутим, како из списа произилази да се у конкретном случају не ради о простом коришћењу платне картице на којој нема покрића, већ о злоупотреби и изигравању рачунарског система у намери прибављања противправне имовинске користи и наношења штете банци чији је комитент окривљени, то по налажењу овог суда, основано се жалбом јавног тужиоца указује да у конкретном случају није било места доношењу побијаног решења.“* (Решење Апелационог суда у Београду, Кж2 По3 15/2011 од 30. 5. 2011. године).

Наведено решење Апелационог суда у Београду илуструје колико кривично дело рачунарске преваре у пракси може бити слично са неким другим кривичним делима када је реч о елементима бића, што све треба имати у виду приликом правне квалификације одређеног кривичног дела.

Занимљив је и случај Румуна Лаурентиу Кристиан Буска (26), који је осуђен марта 2013. године на затворску казну у трајању од 5 година због фишинг превара (облика крађе идентитета), чије су жртве клијенти америчких компанија и финансијских институција. Буска је, заједно са својим саучесницима, слао поруке путем електронске поште у име компанија PayPal, eBay, Comerica Bank, Regions Bank, LaSalle Bank, Well Fargo, Citibank, Capital One, Bank of America и JP Morgan Chase, којим је клијенте ових компанија обавештавао да постоји проблем са њиховим рачуном и да треба да посете сајт на коме треба да оставе своје личне податке, укључујући и

податке као што су бројеви платних картица, датум истека картице, ПИН-ови, имена, адресе, бројеви телефона, и бројеви социјалног осигурања. Тако прикупљене информације, преваранти су касније користили за приступ рачунима и извлачење новца и то најчешће са банкомата у Румунији. Претпоставља се да је Буска у периоду од 2004. до 2006. године на овај начин украо 10.000 бројева дебитних или кредитних картица, а поред њега још 18 држављана Румуније оптужено је за саучесништво у овом случају (Вилић, 2016: 120).[3] Овај случај илуструје несагледиве последице које могу изазвати различити облици интернет превара.

Један од најпознатнијих облика интернет преваре је „нигеријска превара". О овом, али и другим облицима превара на интернету, биће више речи у наставку рада.

### *2.1. „Нигеријска превара" и други облици интернет превара*

„Нигеријска превара" је посебан облик интернет преваре. Извршиоци овог кривичног дела настоје да злоупотребе непажњу и наивност жртве како би стекли противправну имовинску корист. У Србији је, према подацима Тужилаштва за високотехнолошки криминал, први случај стандардног облика ове преваре у нашој земљи пријављен 2009. године, кад је један грађанин остао без 2.500 долара, а од тада је још неколико њих остало без позамашне своте новца. Принцип је углавном код свих починилаца исти. Из иностранства се пошаље „бланко" мејл на неколико хиљада адреса и чека се жртва.

У поруци је изражена молба за помоћ у пребацивању новца из Сенегала или неке друге земље из Африке. Нигерија је била прва земља одакле су жртвама били слати захтеви, па се и по томе превара назвала „нигеријска превара". Пошиљаоци оваквих мејлова углавном се представљају као рођаци неких од званичника или државника страних земаља, који увек желе да пребаце велике своте новца, за шта им је потребан банковни рачун из друге земље, а заузврат обећавају одређену провизију. Преваранти користе Google Translate за превођење порука на српски језик.[4] Много граматичких и стилских грешака се јављају у овим порукама које се путем електронске поште шаљу потенцијалним жртвама.

3 Више о овом случају видети у тексту *Информација – сазнајте више о компјутерској безбедности*, http://www.informacija.rs/Sajber-hronika/Pet-godina-zatvora-zbog-fising-prevara.htm, преузето 3. 9. 2018.

4 *Пажња, не шаљите податке, испразниће вам последњу пару са рачуна,* http://www.kurir.rs/vesti/drustvo/1615127/paznja-nigerijska-prevara-ne-saljite-podatke-ispraznice-vam-poslednju-paru-sa-racuna, преузето 20.7.2018.

Још један пример „нигеријске преваре“ представља и порука следеће садржине: *„Треба ми хитна помоћ. Добар дан. Знам да вам ова пошта може доћи као изненађење. Молим вас, немојте се љути на мене што сте примили моју пошту. Узмите ме као своју кћерку или као сестру и видјели вашу адресу е-поште путем онлине пословног именика током моје претраге. поштена особа и контактирао сам те лично, јер сам озбиљно требао вашу помоћ. Моје име је Мари Франк; Ја сам 20 година и једина дијете мојих покојних родитеља. Мој отац је дуги низ година радио са предузећем за нафту и гас, а он је депоновао збир. (2.000.000 евра) у моје име пре него што је умро 2014. године. Током овог депозита, мој отац је имао сагласност са банком да новац неће бити директно дат до мене све до 25 година или више. Молим вас, хоћете да ми помогнете да пребацим овај новац на ваш банковни рачун за инвестиције и да вам помогнем да дођем у вашу земљу да наставим са школовањем јер мој ујак жели да ме убије и сакупи мој новац за наслеђе, јер сам ја мала девојчица. Пријавио сам га у локалној полицији моје земље (Обала Слоноваче), али полиција није учинила ништа да ми помогне од тада и мој живот је у великом ризику овдје у мојој земљи. Пишем вам ову пошту из локалног хотела у коме се тренутно кријем за моју сигурност док не одем из своје земље након преноса. Ја сам вољан да вам понудим 20% укупних средстава као надокнаду за вашу помоћ након трансфера и желим да ми хитно одговорите ако прихватите да ми помогнете да вам пошаљем више детаља.“*[5] Ова порука представља класичан пример покушаја нигеријске преваре и садржи све њене кључне елементе (апел за помоћ, обећање финансијске надокнаде за извршену услугу, измишљено име пошиљаоца, захтев за достављање података потребних за извршење финансијске трансакције, коришћење компјутерских програма за аутоматско превођење текста итд.). Најбоље је не отварати овакве поруке јер долазе од непознатог пошиљаоца или их обрисати одмах по пријему.

Постоје и други облици превара на интернету. У најчешће вршене интернет преваре спадају и преваре путем интернет промоција, кредитних картица, пирамидалне новчане преваре путем мулти левел маркетинга, пословне понуде и поготово рад од куће, инвестиционе преварне шеме попут „како се лако обогатити”, преваре са путовањима, као и преваре коришћењем туђих бројева здравственог осигурања (Вилић, 2016: 204).[6]

5 Ову поруку је, путем електронске поште, добио аутор овог рада дана 7. августа 2018. године. Како би се очувала њена аутентичност, нису учињене никакве измене у овој поруци.

6 Видети детаљније *Computer Crime Research Center: Fraud in the Internet*, http://www.crime-research.org/articles/Internet_fraud_0405/, преузето 2. 9. 2018.

Различити „бели магови“, лажни послодавци који нуде примамљиве послове у иностранству, девојке са сајтова за упознавање – само чекају своје лаковерне жртве. До преваре путем интернета може доћи и приликом „онлајн“ куповине различитих производа. Купци из незнања или неинформисаности најчешће унапред уплаћују уговорену цену, а до испоруке уговореног предмета никад не дође.[7] Интернет окружење омогућава извршиоцима кривичних дела преваре да делују практично несметано. Лажни профили на сервисима за продају различите робе им омогућавају да прикрију свој идентитет, што отежава откривање ових кривичних дела и њихових учинилаца. Због тога специјализована одељења за борбу против високотехнолошког криминала при Вишем јавном тужилаштву у Београду и Вишем суду у Београду имају веома значајну улогу у сузбијању овог веома софистицираног облика криминалитета. Надлежност наведених државних органа је дефинисана посебним законом.[8] Тужилаштво за високотехнолошки криминал гони учиниоце кривичних дела чија су мета или средство извршења рачунари (односно „сваки електронски уређај који на основу програма аутоматски обрађује и размењује податке“), рачунарски системи, рачунарске мреже, рачунарски подаци, рачунарски програми и ауторска дела која се могу употребити у електронском облику. Све кривичне пријаве које се односе на неко од тих кривичних дела, било коме да су упућене (грађани их најчешће упућују полицији), завршавају у овом органу.[9] Ниједан законски текст ма колико свеобухватан био не може да предвиди и пропише све случајеве који се могу појавити у свакодневном животу. Зато посебну улогу у сузбијању превара у виртуалном свету има превенција. О неким практичним питањима превенције криминалитета, а посебно превенције рачунарских превара биће више речи у редовима који следе.

## 3. Превенција превара на интернету

Превенција криминалитета је од изузетне важности како би се одржала социјална сигурност и безбедност грађана и њихове имовине. Када је реч о преварама на интернету, од нарочитог су значаја мере примарне превенције. Оне су усмерене на то да до извршења кривичног дела преваре

7 Један од многобројних оваквих случајева описан је и у тексту *Жртва интернет преваре*, http://www.rts.rs/page/stories/ci/story/124/drustvo/1092730/zrtva-internet-prevare.html, преузето 31. 7. 2018.

8 Видети одредбе Закона о организацији и надлежности државних органа у борби против високотехнолошког криминала („Службени гланик РС“, бр. 61/2005, 104/2009).

9 *Коме да се обратите ако сте жртва интернет преваре*?, http://www.prevara.info/index.php?option=com_content&task=view&id=1490, преузето 2. 8. 2018.

уопште не дође Како би се остварио овај циљ, неопходно је креирати савремене и ефикасне мере политике сузбијања криминалитета. Политика сузбијања криминалитета се може схватити као научна и као практична делатност (Јовашевић and Костић, 2012: 18). Неколико практичних савета за кориснике интернета може значајно допринети да се смањи број жртава овог облика преваре.

Како би се смањила могућност да дође до преваре на интернету, важно је предузети следеће активности:

1. Никада не отварати електронску пошту која долази од непознатих пошиљалаца;
2. Не посећивати сајтове сумњивог садржаја;
3. Приликом интернет куповине уверити се да фирма-продавац заиста постоји и послује у складу са позитивним правним прописима (обавезна провера у АПР);
4. Плаћање вршити сопственом платном картицом, што олакшава доказивање да је плаћање извршено, ако дође до преваре;
5. Код аукцијске продаје робе проверити ко је спроводи и да ли то правно или физичко лице легално послује;[10]

Када је реч о тзв. „нигеријским преварама", корисници морају да буду скептични по питању свих особа које им се обраћају као званичници из Нигерије, а траже помоћ у новцу која мора да се уплати у неку страну банку, да не верују обећањима о великим сумама новца које ће им бити исплаћене и да веома пажљиво чувају лозинку свог налога како га неко не би злоупотребио. (Вилић, 2016: 208)

Поштовање наведених правила не представља апсолутну гаранцију да неће доћи до интернет преваре или неког другог облика преварног понашања употребом рачунара и информационих технологија, али умногоме смањује могућност да до тога дође.

## 4. Уместо закључка

Појава интернета је довела до неслућених могућности за пренос и обраду информација. Живимо у ери информција. Готово да се не може замислити свакодневни живот без употребе различитих интернет и

10 *Интернет преваре*, https://sr.wikipedia.org/sr/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%BF%D1%80%D0%B5%D0%B2%D0%B0%D1%80%D0%B5, преузето 30. 6. 2018.

других информационих сервиса који се користе у пословне образовне или информационе сврхе, и управо то виртуелно окружење са мноштвом информација ствара погодне услове за различите противправне делатности. По својој друштвеној опасности посебно се издвајају интернет преваре. Њихова погубност се огледа пре свега у наношењу велике имовинске штете жртвама, на коју се надовезују и тешкоће доказивања и откривања, што је, нажалост, карактеристично и за остале облике компјутерског криминалитета.

У спречавању преварних понашања на интернету кључне су мере примарне превенције – односно да до преваре уопште не дође. Као и код других кривичних дела, за ефикасно и брзо процесуирање њихових учинилаца од изузетне је важности обезбедити што је могуће више доказа који ће се користити у судском поступку против извршилаца преваре. Али кривичноправна репресија је последње средство за превенцију сваког облика криминалитета, па и интернет превара. На крају, уместо закључка, ваљало би истаћи да је подизање свести корисника интернета о значају безбедног коришћења интернета најбољи одговор на компјутерски криминалитет. Чини се да старо начело римског права *neminem laedere* и у виртуалном простору треба да остане главна водиља деловања и понашања корисника рачунара.

**Литература/References**

Вилић, В. (2016), *Повреда права на приватност злоупотребом друштвених мрежа као облик компјутерског криминалитета, докторска дисертација*, Ниш: Правни факултет Универзитета у Нишу.

Димовски, Д. (2010), Компјутерски криминалитет, *Зборник радова Правног факултета у Нишу*, год. 55, стр. 195–207.

Јовашевић, Д. (2006), *Лексикон кривичног права*, Београд: Службени гласник.

Јовашевић, Д., Костић, М. (2012), *Политика сузбијања криминалитета*, Ниш: Центар за публикације Правног факултета.

Комлен Николић, Л., Гвозденовић, Р., Радуловић, С., Милосављевић, А., Јерковић, Р.,

Живковић, В., Живановић, С., Рељановић, М. и Алексић, И. (2010), *Сузбијање високотехнолошког криминала*, Београд: Удружење јавних тужилаца и заменика јавних тужилаца Србије.

Константиновић Вилић, С., Николић Ристановић, В. и Костић, М. (2012), *Криминологија*, Ниш: Центар за публикације Правног факултета у Нишу.

Мирић, Ф. (2017), Вршњачко насиље на Интернету кроз призму криминалне феноменологије, у: Д. Димовски, М. Костић и Ј. Станојевић (ур.), *Изазови одрастања у свету савремених технологија*, Ниш: Правни факултет Универзитета у Нишу, Центар за социјални рад „Свети Сава“, Ниш, стр. 55–67.

Закон о организацији и надлежности државних органа у борби против високотехнолошког криминала („Слижбени гланик РС“, бр. 61/2005, 104/2009).

Кривични законик („Службени гласник РС“, бр. 85/2005...94/2016).

Решење Апелационог суда у Београду, Кж2 По3 15/2011 од 30. 5. 2011. године.

*Коришћени електронски извори*

*Computer Crime Research Center: Fraud in the Internet*, http://www.crime-research.org/articles/Internet_fraud_0405/, преузето 2. 9. 2018.

*Paragraf Lex,* рачунарска база правних прописа и судских одлука.

*Жртва интернет преваре*, http://www.rts.rs/page/stories/ci/story/124/drustvo/1092730/zrtva-internet-prevare.html, преузето 31. 7. 2018.

*Интернет преваре*, https://sr.wikipedia.org/sr/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82_%D0%BF%D1%80%D0%B5%D0%B2%D0%B0%D1%80%D0%B5, преузето 30. 6. 2018.

*Информација – сазнајте више о компјутерској безбедности*, http://www.informacija.rs/Sajber-hronika/Pet-godina-zatvora-zbog-fising-prevara.htm, преузето 3. 9. 2018.

*Коме да се обратите ако сте жртва интернет преваре*?, http://www.prevara.info/index.php?option=com_content&task=view&id=1490, преузето 2. 8. 2018.

*Пажња, не шаљите податке, испразниће вам последњу пару са рачуна,* http://www.kurir.rs/vesti/drustvo/1615127/paznja-nigerijska-prevara-ne-saljite-podatke-ispraznice-vam-poslednju-paru-sa-racuna, преузето 20. 7. 2018.

***Filip Mirić, LL.D.***
*Associate for Post Graduate Studies, Faculty of Law,*
*University of Niš*

## *INTERNET FRAUD AS A FORM OF CYBERCRIME*

***Summary***

*The development of the Internet has contributed to a faster and easier transfer and greater availability of information. Unfortunately, an increasing number of Internet users and services have also resulted in the increase of various cyber crimes. Fraud is one of the most common and prominent property-related crimes committed on the Internet. In this paper, the author presents and discusses the basic criminological and criminal law characteristics of Internet fraud as a form of cyber crime. Focusing on the criminal regulation of the Republic of Serbia, the author discusses the similarities and differences between the traditional criminal offense of fraud and the computer fraud that can be committed on the Internet. In illustration, the author elaborates on the emergence and modus operandi of the fraudulent scheme known as the "Nigerian Scam" (advance-fee fraud), considering that many Serbian citizens fell victim to this type of fraud. The author underscores the importance of primary prevention aimed at combating Internet fraud and provides advice how to preclude victimization and thus contribute to reducing the prevalence of the cyber crime.*

***Keywords****: Serbian criminal legislation, crime against property, fraud, cyber crime, prevention.*