UDK:173.1:393.72
Biblid 1451-3188, 9 (2010)
Год IX, бр. 31–32, стр. 151–163
Изворни научни рад

др Владимир УРОШЕВИЋ[1]

„КЛИК" ПРЕВАРЕ

ABSTRACT

In order to profit from the services provided to customers, the owners of Internet sites often rent space on those sites to a number of interested persons or companies for advertising. Rising of manipulation with "Pay-per-Click" advertising threw its abuse as spouted on the Internet. The essence of this manipulation lies in the fact that payments to the owner of the website on whose pages ads are published are calculated according to the number of user visits, which, in fact, were completely artificially generated. Such a fraud is known as the "Click fraud". The danger that threatens from this type of fraud is great as they may jeopardize the work of many companies whose commercial activities rely on the profits through Internet. Systems for prevention of this type of a fraud are still not sufficiently effective. The number of Internet users in the Republic of Serbia is growing rapidly and it is expected that the number of companies that use Internet to promote their products and services will increase. This type of fraud is a serious threat to the contemporary advertising and because of that fact the author devotes special attention to the effective prevention of this phenomenon in the future.

Key words: "Click" fraud, *Pay-Per-Click*, high technology crime, malignant software, computer fraud.

I) УВОД

Појава Интернета, а посебно *World Wide Web*-а утицала је револуционарно на многе аспекте савременог живота. Данас људи, захваљујући Интернету и сервисима који се на њему налазе, могу међусобно да комуницирају са било које тачке на планети. Ова појава променила је начин размишљања савременог човека, као и начин пословања. Поред тога што је погодно средство за комуникацију, Интернет

[1] МУП Републике Србије. E-mail: vladimir.urosevic@mup.gov.rs.

је и веома богат извор различитих врста података и информација. Од појаве Интернет претраживача, велика количина информација постала је лако доступна корисницима Интернета широм света. Највећи број информација и услуга на Интернету које се пружају корисницима од стране различитих сервиса најчешће је потпуно бесплатан. Међутим, онај ко ове информације омогућава и објављује, мора са друге стране, да плати одређене трошкове који настају при објављивању. Како би остварили профит од услуга које пружају крајњим корисницима, власници Интернет сајтова често изнајмљују „простор" на својим Интернет страницама заинтересованим лицима, предузећима или организацијама за рекламирање. Овакав начин покривања трошкова који настају стварањем *On line* сервиса данас је најчешћи. Најпознатији феномен овог типа је Интернет сервис *Google*. Овај Интернет претраживач донео је својим власницима веома велики профит, захваљујући омогућавању рекламног простора компанијама, који се налази непосредно поред резултат претраге који се приказује крајњем кориснику који врши претраживање преко овог сервиса. Дакле, поред телевизије, радија и штампе, рекламирање на Интернету постаје све важније за велики број клијената пошто се број корисника Интернета свакодневно повећава. Извршиоци кривичних дела увек, у свакој пословној грани, покушавају злоупотребама да остваре противправну имовинску корист или да некоме нанесу штету. На Интернету је примећено појављивање већег броја злоупотреба манипулацијом тзв. *Pay-Per-Click* рекламама, чија је суштина плаћање власнику Интернет сајта на чијим страницама је објављена реклама, по једној посети корисника, које су у ствари вештачки генерисане. Овакве преваре познатије су као „клик преваре" (*Click fraud*).[2] Преваре у суштини није тешко извршити, а опасност која од њих прети је велика, пошто на овакав начин могу да угрозе рад многих компанија чије се комерцијалне активности највише ослањају на стварање профита преко Интернет мреже. Системи за борбу против ове врсте превара још увек нису довољно ефикасни, како када је откривање оваквих превара у питању, тако и у случају њиховог спречавања.

[2] Корисник Интернета при посетама Интернет страницама на којима се налази одређена реклама њу види у облику Интернет линка или банера, а кликом тј. одласком на линк или банер и кликом помоћу рачунарског уређаја – миша бива усмерен на Интернет страницу оглашивача рекламе. Након што мишем кликне на линк настаје обавеза оглашивача да исплати уговорену суму власнику Интернет сајта на чијим страницама је објавио свој линк, банер и сл. Та обавеза најчешће се обрачунава према укупном броју посета у одређеном временском раздобљу.

II) ПОЈАМ КЛИК ПРЕВАРЕ

У прошлости, *On line* рекламирање заснивало се на тзв. *Cost-Per-Impression* (плаћање по основу утиска који корисник има о реклами) моделу наплате за рекламирање. Цена рекламирања се наплаћивала по принципу *Cost Per Mile* („цена по пређеним миљама" на енглеском језику), који практично представља цену на сваких 1000 коментара одређене рекламе од стране корисника Интернета. Метода је била заснована на моделу који је примењиван на телевизији и у штампи, где је клијенту који рекламира своје производе услуга била наплаћивана на бази броја појављивања рекламе која је објављивана, у одређеном временском периоду. Овај модел је био омиљен међу власницима Интернет сајтова због тога што су услуге наплаћиване без обзира на учешће корисника и ефекете које реклама код њих изазива. На Интернет претраживачима компанија као што је *Google* почеле су да се примењују тзв. *Pay-Per-Click* модели за *On line* рекламирање на Интернету. Поменути тип „аранжмана" подразумева да она лица или предузећа која се рекламирају на одређеном Интернет сајту плаћају ономе ко објави њихову рекламу за сваку посету од стране корисника Интернета који је на рекламу (нпр. преко линка или банера) кликнуо, и затим био усмерен на Интернет сајт компаније. Дакле, методом се врши се наплата на основу активности корисника везаних за рекламу. Овакав начин рекламирања је омиљен међу оним клијентима тј. компанијама које желе да привуку кориснике преко својих реклама како би, доласком на њихов Интернет сајт платили одређене услуге, извршили наручивање или куповину одређене робе и сл. На *Google* – овом претраживачу по систему *AdWord* оглашивачи реклама се путем аукција опредељују на основу којих ће се кључних речи у резултатима претраге појавити њихова реклама. Њихова реклама се појављује одмах поред резултата претраге од стране корисника на Интернет претраживачу, и то на основу задате кључне речи од стране корисника. Поменута форма рекламирања познатија је као „спонзорисана претрага". Очигледна корист за оглашивача рекламе је та што је корисник који види рекламу већ заинтересован за тему која је везана за кључну реч (пошто је ту кључну реч и унео у поље за претраживање и покренуо претрагу), и самим тим постоји већа шанса да ће такође бити заинтересован и за производ или услугу која се рекламира поред добијених резултата претраге. На пример, кориснику који тражи резултате на основу кључне речи „сат" може се у пољу за рекламирање приказати реклама произвођача *Fossil*. Корисници Интернета такође имају корист од такозваног „циљаног рекламирања",

пошто се преко њих приказују само оне рекламе за производе за које је су највероватније и заинтересовани. По систему *AdSense* фирме *Google*-а, на сличан начин као и по систему *AdWords*, након што се оглашивачи рекламе определе за рекламу која ће се појавити на основу кључне речи, на основу анализе садржаја Интернет сајта, фирма *Google* смешта рекламу на Интернет сајт који има сличан садржај који је повезан са том кључном речи. Сваки пут када неко кликне на ту рекламу власник Интернет сајта добија проценат од зараде коју *Google* као фирма оствари од оглашивача рекламе, тако да практично фирма *Google* зарађује само део тог новца, односно провизију.

Са овог аспекта разликују се два типа превара: преваре од стране учесника и преваре од стране објављивача. Први вид преваре најчешће се не врши ради стицања противправне имовинске користи, пошто ње заправо и нема, већ у намери да се оштети или сузбије пословна конкуренција. Превара се везује најчешће за рекламе које се објављују по систему *AdWords*, када конкуренција врши превару према конкурентској фирми која је објавила рекламу. Извршилац, знајући да сваки клик на рекламу кошта његову пословну конкуренцију доста новца, смишља превару у оквиру које ће на одређеном Интернет сајту где је реклама објављена она бити вишеструко пута посећена, понекад и аутоматским путем, вештачки преко *botnet*-а, чиме се наноси велика материјала штета, пошто заправо нема користи која настаје када се врше праве посете рекламама од стране корисника. Поменути напади често се врше од стране пословне конкуренције коришћењем савремених рачунарских метода из области високотехнолошког криминала. Метода преваре од стране оглашивача врши се од стране лица које је објавило рекламу, тј. од стране самог власника Интернет сајта где је реклама објављена (или где је објављено више реклама). То власници Интернет сајтова где су објављене рекламе чине са унапред смишљеном идејом: да остваре противправну имовинску корист вршењем кривичног дела рачунарске преваре на штету својих клијената који су код њих објавили рекламу. Пошто лице, компанија или нека друга организација која објављује рекламу власнику Интернет сајта плаћа за сваку посету реклами од стране корисника, власнику Интернет сајта је у интересу да рекламу коју је објавио преко њега посети што више корисника. Извршиоци кривичних дела на чијим су Интернет сајтовима објављене рекламе вештачки повећавају број оваквих посета у жељи да зараде више новца. Најпростији облик оваквих превара своди се на то да се ангажују различита лица која ће посећивати рекламе. На Интернету постоји много Интернет сајтова и сервиса који пружају могућност за упознавање,

дружење и забављање.[3] И ову могућност извршиоци кривичних дела користе како би ангажовали лица за помоћ при извршењу клик превара. Професионалци у области високотехнолошког криминала ангажују велики број лица која се овим послом баве организовано, или који користе аутоматизоване методе за посету. Облик у коме се користи аутоматизовање посета је најтежи и најопаснији, пошто производи велики број напада у кратком временском року. Најтежи проблем при вршењу ових кривичних дела је утврђивање да ли се ради о правим или лажним посетама које су вештачки генерисане. Преваре од стране власника Интернет сајтова на којима су објављене рекламе најчешће представљају класичне злоупотребе поверења, као и кршење уговорних обавеза. Иако се у многим уговорима овог типа правно регулишу права и обавезе оглашивача и власника Интернет сајта који рекламира производе или услуге, међу којима су и спречавање коришћења аутоматизованих и организованих посета, као и вештачки генерисаних посета, овај проблем још увек није адекватно решен, посебно када се у обзир узме глобална природа Интернета и начин његовог функционисања (принципи функционисања као мреже која нема власника, анонимност корисника и сл.).

Компанија *Google* може да послужи као одличан пример како би се виделе размере ове врсте рачунарске преваре. Рекламирање на Интернету данас је многим компанијама заступљено као 99% решење за рекламирање, а комерцијале активности многих Интернет сајтова изражавају се у милионима и милијардама долара. Ако се ова врста преваре у скорије време не реши и не прекине, овакав облик наплате рекламирања би могао да буде угрожен. Сама чињеница да се сервис *Google* са зарадом од 6,7 милијарди долара у 2005. години повећао на 10,4 милијарди долара у 2006. години говори о размерама овог посла и његовом значају. У 2006. години 60% ове зараде је је потицао од сервиса *Google AdWords*, система који је иначе подложан преварама од стране конкурентских фирми, а осталих 40% од сервиса *AdSense*, система подложног преварама од стране власника Интернет сајтова који објављују рекламе (податак из годишњег извештаја за 2006. годину компаније *Google Inc* који је објављен 2007. године). Поред сервиса за претраге, *Google* је у наведеним годинама, као и многи други Интернет сервиси који се баве оваквим видом рекламирања, драстично

[3] В. Урошевић, З. Ивановић, „Улога интернета код ангажовања посредника у преузимању противправно прибављене робе и новца извршењем кривичних дела високотехнолошког криминала", *Гласник права,* Правни факултет Универзитета у Крагујевцу, 2010, бр. 1, стр. 88.

увећао свој профит. Иако се број клик превара још увек не може тачно проценити, студије које су изведене указују на то да је око 14% оваквих активности заправо лажно.[4] Према *Bernard J. Jansen*-у, ванредном професору Државног универзитета у Пенсилванији из Одељења за компјутерски инжињеринг, не може се тачно рећи колика је тачност Интернет претраживача при филтрирању лажних посета путем генерисаних кликова на линкове реклама, али се може закључити да је она око 80% или више, те да то води до закључка да лажне посете чине око 6% од свих посета рекламама преко Интернет претраживача.[5] Компаније као што је *Google* практично имају само два избора како би избегле ову опасност. Прво, могу да отворе нове сервисе у намери да избегну да буду економски зависне од клијената који рекламирају своје производе преко њихових Интернет сајтова, или да предузму одређене кораке како би превентивно деловали, пре него што настане штета. Без обзира на то које се техничко решење примењује, потребно је што боље разумети начин извршења овог вида кривичног дела рачунарске преваре како би јој се адекватно супротставило на свим нивоима.

III) НАЧИНИ ИЗВРШЕЊА КЛИК ПРЕВАРА

Клик преваре врше се на више различитих начина, и то такозваним „симолованим кликом", нападима преко *Botnet* мрежа, пребацивањем скрипти тј. злонамерних рачунарских програма на рачунаре посетиоца које затим покрећу поновне посете Интернет сајтовима и симулирају прави клик корисника на основу предходне посете реклами. Сви начини извршења су веома специфични, па их је потребно објаснити појединачно и детаљније.

Симуловани „клик"

Суштина оваквог начина извршења кривичног дела је у томе да се ради о аутоматизованом процесу који доводи до симулацији клика на одређену рекламу, тј. Интернет линк где се она налази. Како би се разумео принцип функционисања ове врсте преваре, прво се мора разумети принцип функционисања технологије која подржава рекламу на Интернет сајту тј.

[4] E. Mills, "Study: Click fraud could threaten pay-per-click model", Интернет: http://www.news.com/Study-Click-fraud-could-threaten-pay-per clickmodel/2100-1024_3-6090939.html, 22/03/2010.

[5] B. Jansen, *Click Fraud, Webtechnologies*, The Pennsylvania State University, 2007, p. 102.

технички принцип њеног функционисања. Типични Интернет сервиси за *On line* рекламе функционишу на тај начин што обезбеђују власницима Интернет сервиса одређене кодове написане у *JavaScript* програмском језику, како би их поставили на Интернет странице свог Интернет сајта. Ови кодови се затим покрећу у оквиру Интернет претраживача који корисник користи и врше преузимање рекламе са рачунарског сервера на коме је она постављена у реалном времену. Покретачи преузимања затим врше трансфер кодова који су у *JavaScript* формату у *HTML* формат (практично мењају врсту програмског језика, а садржај рекламе остаје исти), како би се реклама појавила у облику који је потребан да би је корисник видео. Када корисник посети Интернет линк рекламе, подаци о томе практично пролазе преко сервера, дајући тако прилику власнику Интернет сајта да региструје број посета, и касније на основу тога наплати своје услуге власнику рекламе. Након тога корисник се пребацује тј. редиректује на Интернет сајт где се налази реклама.[6] Евидентно је да програм који симулира клик корисника мора да функционише и врши одређене функције као претраживач. Прво мора да изврши *JavaScript* код који повлачи потом *HTML* код Интернет странице где се налази реклама, да пребаци ове *HTML* кодове у потрази за Интернет линком, и потом да пошаље *HTTP* захтев серверу на коме се налази *WEB* страница на одређеној *URL* адреси.

Клик превара преко *Botnet* мрежа

Симуловање клика је у суштини прилично лако. Откривање основног вида овакве преваре је понекад и јасно уочљив анализом логова на серверима. Разлог за то је следећи: када програм пошаље *HTTP* захтев према серверу онога ко је поставио рекламу *IP* адреса рачунара корисника практично се у логовима појављује као захтев за пребацивање конекције између клијента и сервера. Практично све што треба да се открије да је извршена клик превара је провера лог фајлова, посебно са освртом на оне фајлове где се појављује једна *IP* адреса са великим бројем захтева за конекцију. Како би избегли да их на овај начин открију, извршиоци кривичних дела често ангажују *botnet* мреже рачунара који су под њиховом контролом, или плаћају извршиоце других кривичних дела који имају велики број заражених рачунара под својом контролом да за

[6] M. Gandhi et al., "Badvertisements: Stealthy click-fraud with unwitting accessories", *Journal of Digital Forensic Practice*, Taylor & Francis, 2006, no. 2, pp. 131-142.

одређену суму новца преко тих рачунара врше клик преваре. Овакве мреже се понекад састоје од неколико хиљада рачунара који су заражени тзв. злоћудним програмима, који су сви под контролом извршиоца кривичног дела.[7] Овакве мреже настају на тај начин што извршиоци кривичних дела преузимају контролу на рачунару и потом преко мреже врше контролу рачунара и задају одређене задатке које рачунари извршавају на њихов знак тј. извршни код који је унапред одређен од стране извршиоца кривичног дела.

Преузимање рачунара

Рачунари се веома често компромитују од стране извршилаца кривичних дела кроз експлоатисање сигурносних пропуста и слабости рачунарског система (лоше антивирусне заштите, пропуста и оперативним системима и сл). Програм који врши истраживање ових пропуста и слабости најчешће се назива као *exploit* (на енглеском језику, а слободан превод би био „истраживач"). Извршиоци кривичних дела ове програме некада пишу сами или, што је веома чест случај користе већ познате програме овог типа који су написани за познате сигурносне пропусте који су доступни на Интернету (најчешћи су они везани за сигурносне пропусте у оперативним системима *Microsoft Windows*). Када се одлучи за одређени тип злоћудног програма извршилац кривичног дела почиње да скенира одређени опсег *IP* адреса у потрази за рачунарским системом који испуњава услове за употребу злоћудних програма тј. за оним системом који има одређену верзију оперативног софтвера или неки други рачунарски програм који је погодан за напад и експлоатисање. Када се открије слабост система користи се злоћудни програм типа *exploit* да се добије даљински приступ рачунару (*remote access*) и како би се остварила контрола над њим. Након што *exploit* пронађе сигурносне пропусте у рачунарски систем се убацује малициозни програм - вирус који након тога преко унапред задатих команди контактира рачунар који контролише читаву мрежу заражених рачунара тј. *botnet* мрежу, са којег се задају команде за контролу и за давање инструкција тј. задатака зараженом рачунару.

[7] S. Soubusta, "On Click Fraud", *Informationswissenschaft &Praxis*, Düsseldorfer Informations wissenschaft, 2008, no. 59, pp. 136-141.

Начин контроле и задавања команди рачунарима заражени рачунарским вирусом (*Comand&Controle* функција)

У највећем броју случајева за контролу и задавање команди користе се *IRC* (*Internet Related Chat*) сервиси и њихови канали комуникације. Ови сервиси се најчешће састоје од једног или више сервера који служе за размену порука и/или команди за повезивање између клијента. Преко ових сервиса власник мреже заражених рачунара може преко канала за комуникацију једновремено и централизовано да зада команду сваком зараженом рачунару преко унапред задатих параметара и команди, да пошаље и покрене рачунарски програм на зараженом рачунару који ће даље вршити клик преваре са зараженог рачунара на Интернет сајту где се налази циљана реклама. Алтернативни начин контролисања мреже заражених рачунара је и употреба корисничког интерфејса преко којег се заражени рачунар конектује на рачунарску мрежу. Ова метода је јако захтевна пошто злоћудни програм при конекцији захтева *update* тј. посету серверу који контролише заражене рачунаре, како би пријавио да се заражени рачунар конектовао на Интернет и да се може покренути одређена функција. На овај начин се генерише и већи Интернет саобраћај од и ка зараженом рачунару, па је и могућност откривања већа.

Пребацивање скрипти на рачунаре посетилаца Интернет сајтова

Један од најсофистицираних начина извршења овог типа рачунарске преваре је постављање „скрипти" на Интернет сајтовима на којима се реклама налази и то од стране власника Интернет сајта који врши кривично дело рачунарске преваре. Ове скрипте се аутоматски приликом посете Интернет сајту пребацују на рачунар посетиоца. Скрипта потом покреће активност на зараженом рачунару (без знања корисника рачунара) којом се имитира прави клик посетиоца, иако он то није учинио. *Log* фајлови оглашивача рекламе при таквој посети бележе идентитет посетиоца и његову *IP* адресу на серверу, и на основу тога се касније врши наплата власнику објављене рекламе. Овај начин извршења се ипак може открити и пратити. У случају сумње да се врши овакав вид рачунарске преваре, власник објављене рекламе требао би да посети Интернет сајт оглашивача без посете реклами коју је објавио, те да касније провери да ли су његова *IP* адреса и *ID* број регистровани као да су кликнули на линк рекламе, иако то нису учинили. Међутим, извршиоци кривичних дела веома често знају за овај начин провере од стране власника објављених

реклама, па су смислили начин да избегну да буду откривени. Ово решење подразумева постојање два Интернет сајта, првог који пребацује скрипте и другог који је сасвим регуларан, на коме је објављена реклама. Интернет сајт који не пребацује скрипте је потпуно у реду, и при посети се не може уочити ништа сумљиво. За превару служи други Интернет сајт који није повезан са првим, и над којим извршилац у потпуности има контролу. То може бити Интернет сајт који је извршилац отворио са намером да изврши превару, или Интернет сајт лица које се појављује као саизвршилац, помагач и слично. На други Интернет сајт се поставља скрипта која аутоматски врши учитавање лажне странице која је уствари копије прве, регуларне стране сајта на коме је реклама објављена, и то сваки пут када корисник посети другу Интернет страницу, при чему *IP* адресе остају забележене као да је посета била намењена правој Интернет страници где се налази реклама. Ови напредни начини вршења рачунарских превара постали су претња савременом начину рекламирања на Интернету. Многе организације су веома посвећене безбедносним проблемима и одвајају додатне ресурсе везане за заштиту система, особља, технике и предузимају друге потребне радње како би заштитили информације и рачунарске системе. Иако те активности помажу да се ризик смањи, оне га свакако не елиминишу.[8] Неке од ових мера подразумевају модификацију система наплате по систему наплате по основу активности посетиоца након регистровања посете (нпр. куповина, попуњавање формулара и сл), наплате по једном појављивању рекламе, наплате по проценту појављивања рекламе на основу кључне речи, преко откривања корелација са сајтовима са којих је честа посета преко алгоритама које користе Интернет провајдери, путем дупле провера преко асоцијације са корисницима и остављањем тзв. *cookies*-а којима се детектује индивидуални корисник и сл. Ипак, ниједна од ових мера није довољно ефикасна да заштити власнике реклама од ових врста напада везаних за клик преваре. Интернет је мрежа у оквиру које извршиоци често прикривају свој идентитет користећи његову инфраструктуру, али и пријављивањем података при регистрацији на различитим Интернет сервисима који су измишљени или прибављени крађом података о туђем идентитету. Истраживање кривичних дела у којима је дошло до крађе идентитета на Интернету веома је тешко, посебно када се у виду има чињеница да Интернет не познаје границе, и да докази о извршеним

[8] Nicholas Ianelli, Aaron Hackworth, "Botnets as a Vehicle for Online Crime", *The International Journal of Forensic computer science*, 2007, no. 1, pp. 21, etc.

кривичним делима могу да се налазе на серверима који се налазе у било којој држави на свету. Ову чињеницу посебно треба имати у виду када се ради о нападима преко *botnet* мрежа, чијег је власника јако тешко пронаћи.

IV) ИЗВОРИ

- Gandhi M., et al., "Badvertisements: Stealthy click-fraud with unwitting accessories", *Journal of Digital Forensic Practice* ,Taylor & Francis, 2006, no. 2, pp. 131-142. Jansen B.: Click Fraud, Webtechnologies, The Pennsylvania State University, САД, 2007, стр.102.
- Ianelli, Nicholas, Hackworth, Aaron, "Botnets as a Vehicle for Online Crime", *The International Journal of Forensic computer science*, 2007, no. 1, pp. 21, etc.
- Mills, E., "Study: Click fraud could threaten pay-per-click model", Интернет: http://www.news.com/Study-Click-fraud-could-threaten-pay-per clickmodel/ 2100-1024_3-6090939.html, 22/03/2010.
- Soubusta, S., "On Click Fraud", *Informationswissenschaft &Praxis*, Düsseldorfer Informations wissenschaft, 2008, no. 59, pp. 136-141.
- Милошевић, М., Урошевић, В., „Крађа идентитета злоупотребом информационих технологија", У: *Безбедност у постмодерном амбијенту*, зборник радова књига 6, Центар за стратешка истраживања националне безбедности Београд, 2009, стр. 58.
- Урошевић, В., Ивановић, З., „Улога интернета код ангажовања посредника у преузимању противправно прибављене робе и новца извршењем кривичних дела високотехнолошког криминала", *Гласник права,* Правни факултет Универзитета у Крагујевцу, 2010, бр. 1, стр. 88.

V) ЗНАЧАЈ ЗА РЕПУБЛИКУ СРБИЈУ

Рекламирање на Интернету је уносан посао за власнике Интернет сајтова, а истовремено је и друштвено користан посао пошто омогућава великом броју корисника Интернета да, преко сервиса који се на овај начин финасирају, дођу до података и информација на брз, једноставан и ефикасан начин, најчешће потпуно бесплатно. Са друге стране, великом броју државних институција, невладиним организацијама, удружењима, као и приватном сектору пружа се могућност рекламирања сваки пут када корисник на Интернету тражи одређени садржај, и на тај начин постиже велика вероватноћа да ће погледати и њихов Интернет сајт на коме нуде робу или услуге. *On line* активности везане за рекламирање су многим

компанијама уједно постале и једини начин рекламирања, а Интернет простор заузео је значајно место као медиј за ову врсту реклама. Многи велики Интернет сервиси, као што је *Google*, финансирају се на описани начин, а великом броју ових сервиса то је и једини извор комерцијалних прихода. Међутим, клик преваре су у веома кратком временском року показале да је овај систем веома подложан различитим видовима злоупотреба. Преваре се врло често изводе на веома једноставан начин, али је примећено и коришћење најсавременијих метода из области високотехнолошког криминала, као што је употреба *botnet* мрежа, коришћење скрипти, лажних Интернет сајтова и сл. Због начина извршења ових кривичних дела откривање појединачних случајева је веома тешко, и због тога је потребно константно праћење нових техничко технолошких иновација које омогућавају анализу саобраћаја везаног за кориснике који посећују рекламе и независни систем праћења тог саобраћаја од стране власника реклама. На описане начине овом врстом преваре систем функционисања наплате услуге рекламирања доведен је у питање. У Републици Србији број корисника Интернета у рапидном је порасту, па се очекује и пораст броја компанија које на овакав начин рекламирају своје производе и услуге. Ова врста преваре представља озбиљну опасност и зато је у овом раду феномену клик преваре посвећена посебна пажња, ради ефикасније превенције у будућности. Кривично правни оквири у Републици Србији усклађени су са савременим изазовима када је клик превара у питању и омогућавају кривично правну заштиту од овог начина извршења кривичног дела. У Кривичном законику Републике Србије (објављен у Службеним гласницима Републике Србије бр. 85/2005, 88/2005, 107/2005, 72/2009) кривично дело „Рачунарска превара" предвиђено је у чл. 301, који у ставу један гласи: „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. се наводи, да ће се учинилац казнити затвором од једне до осам година извршилац који делом из става 1. овог члана прибави имовинска корист која прелази износ од четиристопедесет хиљада динара. У ставу 3. се наводи да ће се учинилац казнити затвором од две до десет година ако је делом из става 1. овог члана прибављена имовинска корист која прелази износ од милион и петсто хиљада динара, а ставом 4. је прописано, да ће се извршилац који дело из става 1. овог члана учини само у намери да другог оштети, казнити

новчаном казном или затвором до шест месеци. Клик преваре се могу препознати као специфичан начин извршења кривичног дела „Рачунарска превара из чл. 301 Кривичног законика Републике Србије. Уношењем нетачних података о наводним посетама клијената код најосновинијег облика овог начина извршења, када извршиоци лично, неауторизовано посећују линкове реклама, као и аутоматизованим утицајем на обраду података преко генерисаних посета, лажно се приказују подаци о броју клијената који су посетили рекламу и утиче се на крајњи исход обраде података на основу које се врши наплата власнику рекламе, пошто се вештачки и неосновано повећава број посета корисника, на основу којих се врши наплата власнику рекламе. Код извршилаца ових превара постоји и намера за прибављање противправне имовинске користи за себе или другога, као и намера наношења имовинске штете (нпр. у случајевима напада од стране конкуренције).