UNIVERZA V LJUBLJANI

EKONOMSKA FAKULTETA

DIPLOMSKO DELO

USTVARJANJE IN ODKRIVANJE LAŽNIH KLIKOV V SPLETNEM OGLAŠEVANJU

Ljubljana, marec 2010 **BLAŽ GRGUROVIČ**

IZJAVA

Študent BLAŽ GRGUROVIČ izjavljam, da sem avtor tega diplomskega dela, ki sem ga napisal pod mentorstvom dr. ALEŠA POPOVIČA, in da dovolim njegovo objavo na fakultetnih spletnih straneh.

V Izoli, dne _____ Podpis: _____

KAZALO

KAZALO SLIK

UVOD

Spletno oglaševanje je v tem trenutku najhitreje rastoča vrsta oglaševanja (Soubusta, 2008, str. 138). Vedno več podjetij se odloča oglaševati na spletu, saj je splet v primerjavi z ostalimi mediji veliko bolj fleksibilen in interaktiven ter omogoča natančnejše merjenje učinkov oglaševalskih akcij. Največja slabost spletnega oglaševanja so zlorabe, povezane z lažnimi kliki. Podjetja in posamezniki se poslužujejo vedno bolj zapletenih metod, ki jim omogočajo nelegalno izkoriščanje oglaševalskih sistemov, temelječih na plačilu na klik.

Namen diplomske naloge je analizirati problematiko lažnih klikov na spletne oglase, ki negativno vplivajo na doseganje želenih poslovnih rezultatov spletnega oglaševanja podjetij glede na njihove vložke. Podjetja potrebujejo več informacij o lažnih klikih in načine, kako analizirati svoje spletne oglaševalske kampanje, temelječe na načinu plačila na klik. Tako bi ugotovila ali so bila bremenjena tudi za lažne klike, in se odločila kako ukrepati v takih primerih. Če podjetje ne vzpostavi ustrezne analitike, lahko lažni kliki povzročijo nezaželene odhodke, povezane s spletnim oglaševanjem. Ti lahko oslabijo ali celo prekinejo oglaševalske kampanje.

Cilj diplomske naloge je predstaviti učinkovite ukrepe odkrivanja lažnih klikov, ki omogočajo podjetjem, da ustrezno zavarujejo svoje investicije v spletno oglaševanje. Predstavljeni ukrepi se med seboj razlikujejo in niso vsi primerni za vsako podjetje, ki oglašuje preko spleta. Podjetja z relativno majhnimi vložki v spletno oglaševanje bi se morala odločati za enostavnejše načine, ki ne potrebujejo veliko znanja in investicij, medtem ko bi tista, ki v spletno oglaševanje vlagajo relativno več, morala izbirati naprednejše rešitve, ki pa zahtevajo tudi večje investicije in ustrezne kadrovske zmogljivosti.

Diplomska naloga je razdeljena v štiri poglavja, v katerih skušam čimbolj nazorno predstaviti problematiko lažnih klikov v spletnem oglaševanju. V prvem poglavju predstavljam spletno oglaševanje in njegove značilnosti. Primerjam ga s tradicionalnim oglaševanjem v ostalih medijih in ugotavljam prednosti in slabosti. V nadaljevanju opisujem spletne oglase po njihovi pojavni obliki in vsebinskih značilnostih, na kratko predstavim različne načine oglaševanja na spletu ter opisujem plačilne modele, ki določajo načine plačila oglaševalcev. Med njimi je tudi plačilni model CNK (cena na klik), ki predstavlja eno ključnih okoliščin, ki so privedle do nastanka lažnih klikov. Na koncu tega poglavja je v grobem predstavljen potek manjše spletne oglaševalske akcije.

V drugem poglavju se osredotočim na lažne klike in predstavim pogoje, ki so omogočili, da je prišlo do masovnega ustvarjanja lažnih klikov v spletnem oglaševanju. Izbral sem si trenutno največjo oglaševalsko mrežo Google z njenima oglaševalskima programoma za oglaševalce in ponudnike oglasnega prostora AdWords in AdSense. Na podlagi teh sem predstavil kako in zakaj se ustvarjajo lažni kliki. V tem poglavju prikazujem tudi najširšo delitev ustvarjanja lažnih klikov, ki se deli na lažne klike konkurentov oglaševalca in na lažne klike ponudnikov

oglasnega prostora. V drugem delu poglavja predstavim, zakaj je odkrivanje lažnih klikov pomembno in kako se trenutno zbirajo statistični podatki o celotnem številu lažnih klikov.

Tretje poglavje je namenjeno predstavitvi različnih tehnik, ki se uporabljajo za ustvarjanje lažnih klikov. Podrobneje je predstavljena aplikacija, ki oponaša uporabnika spleta in klika na določene oglase preko prednastavljenih posredniških strežnikov. V nadaljevanju je razloženo delovanje omrežja računalnikov s centraliziranim nadzorom. Opisana je tudi uporaba zlonamerne kode na straneh, kjer se strežejo, oglasi s katero se skušajo okoristiti ponudniki oglasnega prostora.

V četrtem poglavju želim doseči cilj diplomske naloge s predstavitvijo načinov, ki omogočajo podjetjem, da si zavarujejo in uspešneje nadzirajo svoje oglaševalske akcije na spletu. Najprej so predstavljena prizadevanja za odkrivanje lažnih klikov različnih udeležencev spletnega oglaševanja, nato opisujem trenutne metodologije odkrivanja lažnih klikov in nazadnje navajam priporočila za oglaševalce, s katerimi si lahko pomagajo in minimizirajo nepotrebne izgube v spletnem oglaševanju.

1 SPLETNO OGLAŠEVANJE

Dostopnost spleta odločilno vpliva na to, da je spletno oglaševanje in z njim povezane goljufije tako razširjeno. Zaradi velike razširjenosti spleta in spletnega oglaševanja ter dejstva, da je lahko udeleženec v spletnem oglaševanju vsak posameznik ali podjetje, ki ponuja oglasni prostor, je težko nadzirati zlorabe in določiti krivce. Najbolj ranljiv za zlorabe je cenovni model spletnega oglaševanja, ki temelji na plačilu oglaševalca za vsak klik na spletni oglas. Na koncu vrednostne verige pa so podjetja, ki vlagajo velike zneske v oglaševanje in želijo v imeti zameno kar največ konverzij, ki se odražajo kot nakupi izdelkov ali storitev, registracije uporabnikov ipd.

Internet je od svojega nastanka do danes dodobra spremenil ljudi in njihove navade. Omogoča opravljenje različnih storitev od doma ali iz naše pisarne. Komuniciramo lahko z ljudmi, ki so na tisoče kilometrov oddaljeni od nas, prebiramo članke tujih medijskih hiš in še marsikaj bi se znašlo na tem seznamu. Splet je ena najbolj razširjenih storitev, ki se pretakajo preko interneta, in obsega že milijarde spletnih strani. Te strani so eden največjih virov informacij in znanja. Velika prednost spleta je, da je večina storitev brezplačnih, in menim, da je prav zaradi tega danes splet tako popularen.

Brezplačen pa je le z vidika uporabnika, kajti na strani izdelovalcev spletnih strani so stroški prisotni. Te stroške je potrebno od nekod pokriti. Podjetja imajo svoje predstavitvene spletne strani. Stroški, vloženi v razvoj takih strani, so stroški oglaševanja, saj je vsak obiskovalec takih strani tudi potencialni kupec produktov podjetja. Državne ustanove imajo svoje spletne strani, ki so financirane iz državnega proračuna. Veliko pa je takih spletnih strani, ki nudijo določeno storitev in krijejo stroške z oddajo oglasnega prostora na strani. Tak pristop

uporablja večina spletnih strani zato, da lahko pokrijejo stroške razvoja, opravljanja in vzdrževanja spletnih storitev (Soubusta, 2008, str. 136).

V nekaterih primerih pa so prihodki iz naslova spletnega oglaševanja tako visoki, da ne pokrivajo le rednih stroškov, ampak ustvarjajo tudi velikanske dobičke. Primer takega uspeha zgolj z izkoriščanjem internetnega oglaševanja je ameriško podjetje Google. Njihov spletni iskalnik je z oddajo oglasnega prostora in nizanjem pomensko povezanih tekstovnih oglasov k iskalnim zadetkom uporabnika uspel zbrati ogromne količine denarja. Iz preprostega spletnega iskalnika je Google prerasel v eno vodilnih podjetij za razvoj programske opreme v svetovnem merilu.

Opredelitev oglaševanja

Opredelitev spletnega oglaševanja se od vira do vira nekoliko razlikuje, zato v nadaljevanju predstavljam nekaj opredelitev tradicionalnega in internetnega oglaševanja. Spletno oglaševanje je potrebno ločiti od internetnega, saj ta pojma nista sopomenki. V nadaljevanju bom s pomočjo različnih opredelitev skušal predstaviti, v čem se razlikujeta in katere so njune skupne značilnosti.

Oglaševanje opredelimo kot najstarejšo, najbolj vidno in najpogostejšo obliko trženjskega komuniciranja, ki obsega vsako plačano obliko neosebne predstavitve organizacije, dobrin, storitev ali zamisli, ki jo plača naročnik (Belch & Belch, 1999, str. 14).

Oglaševanje je vsaka plačana neosebna oblika prezentacije ali promocije zamisli, izdelkov ali storitev znanega plačnika preko množičnih medijev, kot so časopisi, revije, televizija ali radio (Cerar, 2004, str. 9).

Opredelitev internetnega oglaševanja

Internetno oglaševanje je združevanje in uporaba različnih internetnih tehnologij z namenom doseči določene trženjske cilje (Glossary [SensaCom], 2008).

Internetno oglaševanje je splošen izraz, s katerim opredeljujemo vsako uporabo interneta za preusmerjenje strank k določenim podjetjem. Sem uvrščamo spletno oglaševanje ter oglaševanje preko elektronske pošte. Oglaševanje preko elektronske pošte dostikrat povezujemo z izrazom nezaželena pošta (angl. *spam*) (Terms [Wilsol], 2008).

Ward (2008) opredeljuje internetno oglaševanje kot skupek strategij in tehnik, ki se uporabljajo za oglaševanje izdelkov ali storitev s pomočjo uporabe interneta.

Opredelitev spletnega oglaševanja

Spletno oglaševanje je proces gradnje in konstantnega vzdrževanja odnosov s strankami na podlagi spletnih dejavnosti z namenom izmenjave idej, izdelkov in storitev, ki prinašajo obojestranske koristi (Jenko, 2002, str. 2).

Pojem spletno oglaševanje predstavlja vsako promocijo izdelka ali storitve, ki se izvaja preko svetovnega spleta. Razlogi za promocijo so lahko izboljšanje ugleda podjetja, kontakt s potencialnimi kupci, povečanje prodaje določenega izdelka in podobno. Neposredno pošiljanje elektronske pošte ne spada k spletnemu oglaševanju (Cerar, 2004, str. 9).

1.1 Primerjava spletnega oglaševanja s tradicionalnim oglaševanjem

Svetovni splet se nenehno širi, zato raste tudi obseg spletnega oglaševanja kot sredstva za doseganje specifičnih segmentov populacije. Spletno oglaševanje se razlikuje od tradicionalnega. Za tradicionalno oglaševanje s katerim želimo doseči večji del populacije, so značilni veliki stroški oglaševalskih storitev, razpršeno in nesegmentirano predvajanje ali prikazovanje oglasov. Nekateri mediji klasičnega oglaševanja omogočajo tudi možnost kvalitetne vizualne predstavitve oglasa. Spletno oglaševanje pa omogoča dokaj natančno ciljanje populacij, interaktivnost, možnost klasifikacije uporabnikov spleta (potencialni kupci preko spleta) pri nizkih in lažje obvladljivih stroških oglaševanja (Metwally, Agrawal, Abbadi & Zhengh 2006, str. 241).

Vložki v spletno oglaševanje rastejo hitreje kakor vložki v oglaševanje preko tradicionalnih oglaševalskih medijev, kot so televizija, radio ali časopisi. Analize rasti oglaševanja po različnih medijih kažejo, da rast oglaševanja preko svetovnega spleta kar trikrat presega rast tradicionalnega oglaševanja (Internet Advertising Revenue Report 2007, 2008, str. 13).

Tradicionalni način in način oglaševanja preko spleta se med seboj zelo razlikujeta. V nadaljevanju ju primerjam in navajam njune prednosti in slabosti.

1.1.1 Prednosti spletnega oglaševanja v primerjavi s tradicionalnim oglaševanjem

Prednosti pri doseganju ciljne populacije

- **Oglaševanje po posameznih segmentih populacije in možnost izbire s strani uporabnika** - S spletnim oglaševanjem imamo možnost ciljanja na specifične segmente populacije. Tradicionalno oglaševanje se velikokrat poslužuje tehnike ponavljajočega predvajanja slik in fraz z namenom, da bi privabili pozornost potencialnega kupca in ga s tem prepričali v kakovost proizvoda. Ta tehnika pri spletnem oglaševanju ni potrebna, saj se uporabnik lahko sam odloči, kateri oglas si bo podrobneje pogledal. Tako lahko oglaševalci na oglasu prikažejo samo svojo blagovno znamko, saj vedo, da si bo uporabnik spleta, ki pozna njihove proizvode ali storitve, oglas natančneje ogledal (Mendoza & Alexandrov, 2008, str.2).
- **Velika izpostavljenost oglasu** - Spletni oglas lahko vidi veliko število ljudi po vsem svetu. Tradicionalno oglaševanje je ponavadi omejeno na lokalno okolje.

Stroškovna učinkovitost in večja možnost nadzora porabe

- **Stroški oglaševanja** - Oglaševanje preko svetovnega spleta je stroškovno ugodnejše od klasičnega. Objava kratkega tekstovnega oglasa v večji časopisni hiši v Sloveniji stane 500€ na teden (Cenik oglasov [Delo], 2008). Oglaševanje preko radia in televizije pa zahteva še večje denarne vložke. Po drugi strani pa lahko pri največji slovenski oglaševalski mreži tekstovni spletni oglas stane le 0,2€ za 1.000 potrjenih prikazov in prav tako 0,2€ za posamezen klik na oglas (Cenik [Httpool], 2010).

- **Merjenje ROI** - Spletno oglaševanje omogoča boljše izračune kazalcev dobičkonosnosti investicije (angl. *ROI - return on investments*) za vsako oglaševalsko akcijo. Taki izračuni se pri tradicionalnem oglaševanju težko izvedejo in so povečini zelo nenatančni in dragi. Najbolj razširjen kazalec za merjenje uspešnosti spletnih oglasov je stopnja klikov (angl. *CTR - click through rate*). Kazalnik ponazarja število klikov na oglas v razmerju z njegovimi prikazi. Tako se lahko ugotovi, kakšna je priljubljenost oglasa med uporabniki.

Prikazne značilnosti

- **Interaktivnost** - Možnost dvosmerne komunikacije z uporabnikom spleta. Oglaševalec lahko na podlagi pridobljenih informacij uporabniku spleta ponudi podrobnejše informacije o izdelku ali storitvi, ki ga še posebej zanima, ter pravočasno izvede morebitne popravke oglaševalske akcije. Interaktivnost lahko uporabi tudi pri samem oglasu, saj lahko vanj vgradi manjši vprašalnik ali igro in s tem poveča možnost nakupa. Tradicionalno oglaševanje interaktivne komunikacije ne ponuja. Uporablja se enosmerna komunikacija od oglaševalca k potencialnim kupcem. Interaktivnost oglaševalcem omogoča, da zbirajo podatke o uporabnikih spleta in merijo uspešnost oglaševalskih akcij

- **Količina informacij** - Ko je pozornost uporabnika osvojena, mu lahko oglaševalec ponudi poljubno količino informacij o izdelku ali storitvi, ko ga oglas preusmeri na njegovo spletno stran. Ta značilnost je specifična za spletno oglaševanje in je pri tredicionalnem ne poznamo (Mendoza & Alexandrov, 2008, str. 2).

1.1.2 Slabosti spletnega oglaševanja v primerjavi s tradicionalnim oglaševanjem

Omejitve pri doseganju ciljne populacije

- **Struktura populacije** - Tri četrtine rednih uporabnikov interneta je starih od 10 do 35 let. Uporabljajo ga pretežno dinamični ljudje, ki želijo hitro in učinkovito iskati informacije (MOSS - pomlad 2008, 2008). Tradicionalni mediji imajo enakomerneje razporejen spekter populacije in so zato primernejši medij za objavo oglasov, ki so namenjeni večjemu delu populacije. Tak primer so oglasi političnih strank ali državnih ustanov.

- **Omejene možnosti lokalnega oglaševanja** - Zaradi velike globalne razširjenosti svetovnega spleta je preko njega težko učinkovito oglaševati lokalno. Ko želimo oglaševati v ožji regiji, je smiselnejša uporaba tradicionalnih medijev oglaševanja, ki so tam prisotni.

Tehnične omejitve

- **Razlike v zmogljivostih uporabniških vmesnikov in omrežij** - Spletne strani se do končnega uporabnika prenašajo preko omrežij različnih starosti in zmogljivosti, zato se uporabniške izkušnje razlikujejo. Gre predvsem za razlike v hitrosti prenosa podatkov od uporabnika in do njega, za uporabo različnih spletnih brskalnikov, ki vsak po svoje interpretira podatke s spleta, za pomanjkanje določenih aplikacij, ki omogočajo ogled dinamičnih video-vsebin itd.

- **Izpostavljenost zlorabam** - Svetovni splet je s povezavo v internet dostopen vsakomur. Njegove vsebine in tehnologije so odprte narave, kar pomeni, da lahko vsak posameznik z ustrezno programsko opremo in znanjem na njem ustvarja tako dobre kot tudi slabe vsebine. Primer take zlorabe je tudi ustvarjanje lažnih klikov na spletne oglase. Za tako zlorabo spletnih oglasov se lahko na primer ustvari programsko skripto, ki avtomatično simulira klike na določen oglas, dokler ni porabljen ves denar, ki ga je oglaševalec namenil za prikaz tega oglasa (Mendoza & Alexandrov, 2008, str. 2).

Znanje in razpoložljivost virov v podjetju

- **Redno vzdrževanje spletnega mesta, na katerega so povezani oglasi** - Bistvo večine spletnih oglasov je preusmeritev uporabnika spleta z določene spletne strani na spletno stran oglaševalca. Danes so spletne strani več kot le navadno besedilo v HTML-obliki in je za njihovo vzdrževanje potrebno veliko znanja in časa. Prav tako sta pomembni ažurnost in točnost podatkov, ki jih oglaševalec nudi. Slabo urejene in nekonsistentne strani lahko naredijo na potencialnega kupca slab vtis, kar pomeni v večini primerov odhod uporabnika spleta s take strani in posledično izgubo prihodkov.

1.2 Pojavne oblike oglasov na spletu

Na spletu lahko najdemo različne pojavne oblike oglasov. Najprej so bili to krajši tekstovni oglasi v obliki spletne povezave, ki so uporabnika spleta preusmerili na določeno spletno stran. S tehnološkim razvojem internetnih povezav in svetovnega spleta so se začele uveljavljati oglasne pasice (angl. *banner ad*). Pasice so slike ali kratke animacije različnih formatov, pozicionirane na vrhu ali ob robu spletne strani. Na pregledovanje vsebine spletne strani ne delujejo moteče, lahko pa pokvarijo njen celotni izgled. Kot nadgradnja oglasnih pasic so se pojavili oglasi z bogato predstavitveno vsebino (angl. *rich media ad*). V zadnjem času, ko so se širokopasovne povezave v internet dovolj razširile in je na spletu možno pregledovati veliko video vsebin, so postali smiselni tudi video (angl. *video ad*) oglasi in

oglasi znotraj pretočnih vsebin (angl. *in-stream video ad*). Tovrstne oglase ponavadi srečamo, ko pregledujemo video vsebine informativnih spletnih portalov.

Spletni oglasi se delijo na tri skupine: statične, intruzivne in tekstovne. Statični oglasi imajo na spletni strani stalno določeno mesto, kjer se nahajajo. Oglase, ki se po spletni strani gibljejo ali se nam v določenem trenutku prikažejo, imenujemo intruzivni. Velikokrat vsebujejo obogatene oglasne vsebine. Oblikovno in programsko najenostavnejši so tekstovni oglasi. Obstajajo tudi hibridni oglasi, ki združujejo različne lastnosti iz teh treh kategorij (Moncur, 2008).

1.2.1 Statični oglasi

Statični spletni oglasi so slike ali animacije različnih velikosti, ki imajo rezerviran prostor na spletni strani. Lahko so različnih velikosti, vendar so vselej pravokotne oblike.

Oglasne pasice (angl. *banners*)

Oglasne pasice sodijo med najstarejše oblike spletnih oglasov in so še danes zelo uspešne. Pojavljajo se v različnih velikostih. Vrsto let je prevladovala velikost 468 x 60, kajti ob pojavu oglasnih pasic je imela velika večina uporabnikov zaslone z resolucijo 800 x 600. Računalniška oprema je postala zmogljivejša in dostopnejša. Danes večina uporabnikov spleta uporablja zaslone z ločljivostjo 1024 x 768 in več. Temu so se prilagodili tudi ponudniki oglasnega prostora na spletnih straneh in ponudili možnost objave oglasnih pasic velikosti 728 x 90, ki jim pravimo oglasna tabla (angl. *leaderboard*). Poznamo še pokončne pasice (angl. *vertical banner*), velikosti 120 x 240, in polovične pasice (angl. *half banner*), 234 x 60.

Slika 1 prikazuje primer oglasne pasice, ki se ponavadi nahaja na vrhu ali pod vsebino spletnih strani.

Slika 1: Primer oglasne pasice

Vir: Spletna pasica [Datamation], 25.11.2008.

Tržna analiza podjetja COBUS je na podlagi zbranih podatkov od 1178 anketirancev ugotovila, da pasice z ustrezno grafično podobo lahko učinkovito privabijo pozornost uporabnika spleta. Polovica vprašanih pravi, da si oglas tudi podrobneje ogleda, če je dovolj privlačen. Rezultati ankete kažejo tudi, da kvalitetna vsebina oglasnih pasic pozitivno vpliva na nakupovalne namene ljudi in izboljša splošno mnenje o oglaševanih izdelkih (Pagendarm, Schaumburg, 2001).

Nebotičniki (angl. *skyscrapers*)

Slaba lastnost pasic je, da jih uporabnik ne vidi če je postavljeni v določenem delu spletne strani. To slabost skušajo odpraviti nebotičniki. Nahajajo se ponavadi na desnem robu in se raztezajo po celotni višini spletne strani. Ko uporabnik drsi po strani navzdol, ostaja celoten oglas ali samo njegov del ves čas viden. Glede na namen oglasa so si nebotičniki in navadne pasice enakovredni.

Poznamo dve vrsti nebotičnikov: široki nebotičnik (angl. *wide skyscraper*) in nebotičnik. Široki nebotičnik ima dimenzije 120 x 600 in je najbolj pogost med nebotičniki. Običajen nebotičnik je prav tako kot široki nebotičnik visok 600 zaslonskih pik, vendar v širino meri le 60 zaslonskih pik (Standards, Guidelines & Best Practices, 2008).

Gumbi (angl. *buttons*)

Med gumbe sodijo manjši pravokotniki, ki so lahko postavljeni na manjših prostih delih spletne strani. Lahko so pravokotniki velikosti 120 x 90 ali 120 x 60 ali kvadrati velikosti 125 x 125. Slika 2 prikazuje gumbe, primerne za prikaz pokroviteljev, ki želijo biti na spletni strani sočasno prikazani.

Slika 2: Primeri gumbov na spletnih straneh s pokrovitelji

Vir: Advertise on the [Real estate blog], 25.11.2008.

Čeprav se spletne strani med seboj zelo razlikujejo in jih moramo pri analizi lokacij za postavitev oglasov praviloma obravnavati ločeno, lahko določene lokacije na spletnih straneh prinašajo večje stopnje klikov na oglase. Statistika oglaševalskega programa AdSense podjetja Google je dokazala, da najboljše rezultate dajejo spletni oglasi, postavljeni v sredini, in tisti neposredno nad vsebino. Nekoliko slabše so stopnje klikov na oglasi postavljene na

levem delu spletne strani in na dnu strani pod vsebino. Najslabše se izkažejo oglasi, postavljeni v spodnji desni del strani (Kaiser, 2007).

1.2.2 Vsiljeni oglasi (angl. *intrusive ads*)

Vsiljeni oglasi so dobili ime po načinu prikazovanja na spletni strani. Za pasice, nebotičnike in gumbe je značilno, da se naložijo na začetku na določen prostor na spletni strani, medtem ko se vsiljeni oglasi prikažejo naknadno in prekrijejo vsebino spletne strani. Uporaba vsiljenih oglasov na spletnih straneh mora biti zelo premišljena, kajti tovrsten način oglaševanja je lahko za nekatere uporabnike spleta preveč vsiljiv, kar privede do slabše obiskanosti.

Rezultati analize, ki sta jo opravila Hwang in McMillan (2005, str. 69-80) prikazujejo, da so uporabniki spleta nezadovoljni predvsem takrat, kadar sami ne morejo nadzirati spletnih oglasov in kadar imajo občutek, da se jim le ti nasilno prikazujejo pred vsebino spletne strani in jim onemogočajo brskanje.

Izskočno okno (angl. *pop-up*)

Čeprav izskočna okna lahko obiskovalcu ustvarijo slab vtis o spletni strani, so ena najdražjih oblik spletnih oglasov, saj so zelo opazni. Uporabnik mora izskočno okno, ki se mu je prikazalo, vselej zapreti, če želi nadaljevati s pregledovanjem strani. Ponudniki oglasnega prostora morajo biti pri uporabi takih oglasov previdni, saj lahko poslabšajo obiskanost svojih spletnih strani. Druga težava izskočnih oken je, da si lahko uporabniki namestijo programsko opremo, ki prikaze takih oken onemogoči. Danes uporabnikom spleta niti to ni več potrebno, saj imajo novejše verzije brskalnikov take dodatke že vgrajene. V zadnjem času je izskočnih oken vedno manj, kar narekuje tudi direktiva organizacije IAB (Pop-Up Guidelines, 2009). Slika 3 prikazuje izskočno okno, ki prekrije pregledovano vsebino.

Spodnje izskočno okno (angl. *pop-under*)

Spodnje izskočno okno ima podobne značilnosti kot izskočno, le da se na novo odprto okno prikaže v ozadju in ne moti trenutnega brskanja po spletu. Ponavadi ga opazimo šele, ko zapiramo vsa okna brskalnika. Taka vrsta oglasa ne moti trenutnega pregledovanja strani, lahko pa povzroči počasno delovanje brskalnika, če se nabere veliko spodnjih izskočnih oken. Tehnično gledano je tako okno skorajda identično navadnemu izskočnemu oknu, tako da mu novejši brskalniki, ki imajo vgrajene blokade, lahko samodejno preprečijo prikaz (Moncur, 2008).

Slika 3: Izskočno okno

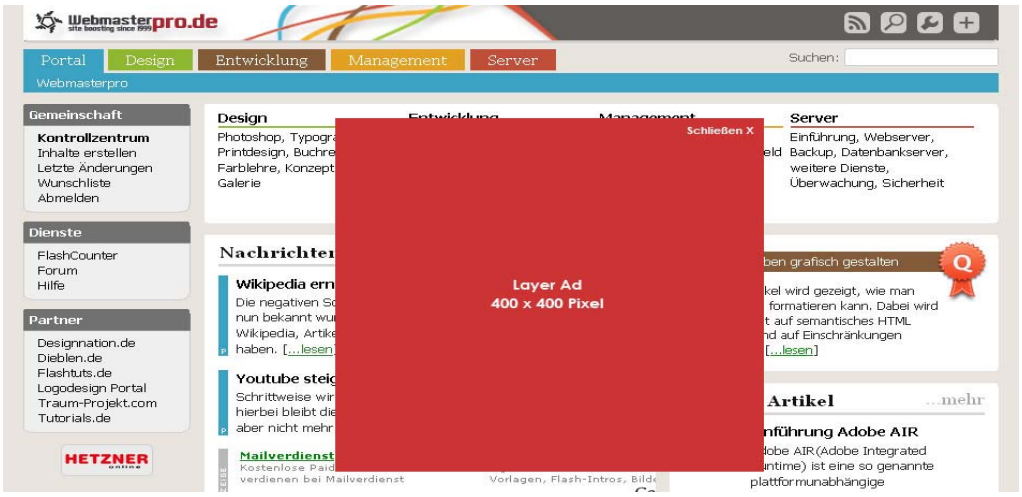
Vir: Manuels Web, 25.11.2008.

Lebdeči oglas (angl. *layer ad*, *floater*)

Novejši brskalniki ne dopuščajo več prikazov izskočnih oken, zato so se na trgu pojavili lebdeči oglasi. Pojavijo se v določenem trenutku in prekrijejo vsebino spletne strani tako, da jih moramo zapreti ali do konca pogledati, če želimo pregledovanje nadaljevati.

Slika 4 prikazuje lebdeči oglas, prikazan nad vsebino spletne strani.

Slika 4: Primer lebdečega oglasa



Vir: Webmaster Pro, 25.11.2008.

Vsebinsko so to obogateni oglasi in vsebujejo video vsebine ali animacije, ki trajajo približno 15 sekund. Po tem času se oglas samodejno zapre oziroma izgine, lahko pa ga že med potekom obiskovalec spletne strani sam zapre (Cerar, 2004, str. 13).

Oglasni premor in celostranski oglas (angl. *interstitial, full-page ad*)

Oglasni premor in celostranski oglas sta si zelo podobna. Razlikujeta se po tem, da se celostranski oglas prikaže samodejno med prebiranjem spletne strani, oglasni premor pa se prične predvajati, ko uporabnik klikne na kakšno povezavo. Oglasa se prikazujeta na celotni vidni površini spletne strani. Tako kot lebdeči oglas sta časovno omejena, uporabnik pa lahko njuno predvajanje v vsakem trenutku ustavi in se vrne na pregledovanje spletne strani. Spletna stran je pod oglasnim premorom ali celostranskim oglasom ves čas vidna, saj jo oglas le zatemni ali zamegli. Ne glede na njuno nastavljeno velikost se oglasa raztegneta čez celotno uporabnikovo vidno polje spletne strani, glede na resolucijo in velikost okna uporabnikovega brskalnika (Moncur, 2008).

Drseči oglas (angl. *slider*)

Posebnost drsečega oglasa je, da ob prebiranju spletne strani navzgor in navzdol oglas sledi uporabniku tako, da ga ima vedno v vidnem polju. Primer drsečega oglasa je prikazan na Slika 5. Oglas sledi uporabniku ob premiku z drsnikom navzgor ali navzdol po spletni strani.

Slika 5: Primer drsečega oglasa

Vir: Anycount, 16.1.2009.

Zamenjava ozadja

Za vnaprej določen čas se celotno ozadje spletne strani spremeni v oglas, ki ga predstavlja slika oziroma grafika. Zamenjava ozadja je primerna za spletne strani, ki ne vsebujejo zapletenih oblikovnih značilnosti in prikazujejo večinoma tekst (npr. iskalni rezultati pri iskalnikih). Po izteku oglasa se uporabniku ponastavi prvotno ozadje spletne strani, takoj zatem tem pa se prikaže opomnik, na katerega ima možnost tudi klikniti in tako obiskati spletne strani oglaševalca (Formati [Iprom], 2008).

Premikajoči oglas

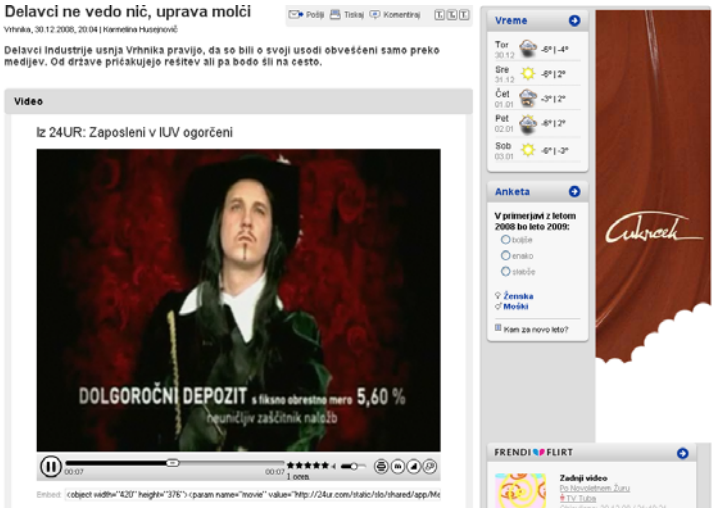
Premikajoči oglas ima značilnosti malega lebdečega oglasa, vendar ga uporabnik ne more zapreti. Lahko se ga premika z uporabo miške. Oglas je lahko časovno omejen ali neomejen (Formati [Iprom], 2008).

Oglasi znotraj pretočnih vsebin (angl. *in-stream video ad*)

Oglasi znotraj pretočnih vsebin se pojavljajo na spletnih portalih, ki ponujajo video vsebine. Oglas se prične predvajati pred vsakim ogledom video posnetka tako, da je potrebno najprej do konca oglas pogledati, če si želimo ogledati izbrani video posnetek. Takih oglasov ne moremo preskočiti ali izklopiti, kot to lahko storimo na primer pri video oglasih v lebdeči obliki. Take vrste oglasov ponavadi srečamo, ko pregledujemo video vsebine informativnih spletnih portalov (Digital Video In-Stream Ad Format Guidelines and Best Practices, 2008).

Primer oglasa znotraj pretočnih vsebin je prikazan na Slika 6.

Slika 6: Oglas znotraj pretočnih vsebin

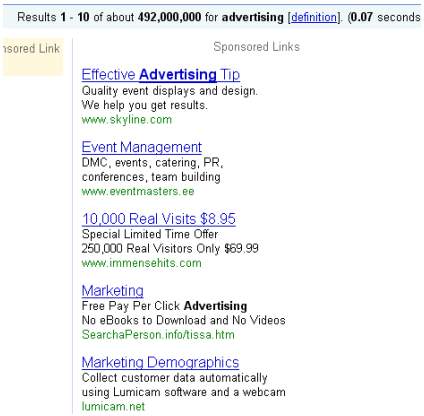


Vir: 24ur.com, 16.1.2009.

1.2.3 Tekstovni oglasi

Prvi so se na internetu pojavili tekstovni oglasi, prikazani na Slika 7. Najpreprostejša oblika spletnega oglasa danes predstavlja velik delež prihodkov iz spletnega oglaševanja. Tekstovni oglasi so ponavadi dolgi od 2 do 5 vrstic in se nahajajo na različnih spletnih straneh. Uporabniki spleta so jih sprejeli bolj kot katerokoli drugo obliko spletnih oglasov.

Slika 7: Tekstovni oglasi



Vir: Iskalnik [Google], 16.1.2009.

1.3 Vsebinske lastnosti spletnih oglasov

Tekst - Tekstovni oglasi so pripravljeni v eni izmed obstoječih pisav. Največkrat so urejeni v slogu, s katerim je urejena tudi ostala vsebina na spletni strani, na kateri se nahajajo. Lahko jim določamo odmike, debelino, velikost, nagnjenost itd.

Slike - Na spletu so razširjene predvsem tri vrste slikovnih formatov, in sicer JPG ali JPEG, GIF ter PNG. Po kakovosti slike je format JPG na prvem mestu, sledi mu PNG, najslabše kakovosti pa so slike v formatu GIF. Kadar kakovost slike ni zelo pomembna se uporablja format GIF, saj zasede malo spominskega prostora na računalniku in ga zato brskalnik prenese hitreje. Formati JPG in PNG fromati zasedejo od 3- do 5-krat več spominskega prostora. V spletnem oglaševanju se slike uporabljajo pretežno v obliki pasic, gumbov ali nebotičnikov.

Animacije - Pojavile so se kot nadgradnja slik. Najdemo jih v pasicah, nebotičnikih ali gumbih v obliki formatov GIF ali Flash. GIF-animacije so preproste zaporedne ponovitve slik, ki tvorijo učinek premikajočih se figur. Animacije Flash so lahko podobno kot GIF le krajše animirane slike, lahko pa so tehnološko veliko zmoglivejše. Oglase z naprednimi Flash animacijami uvrščamo v oglase z obogateno predstavitveno vsebino.

Video oglasi – Predstavljajo spletno posebnost. Ker so širokopasovne povezave v splet dovolj razširjene, so se pojavili video oglasi, ki so so natanko taki kot v televizijskih oglasnih blokih. Lahko se predvajajo v obliki lebdečega in celozaslonskega oglasa ali v obliki oglasa znotraj pretočne predstavitvene vsebine. Največkrat je to lebdeči oglas v obliki pravokotnika (angl. *rectangle*) 300 x 250 ali kvadrata (angl. *square*) velikosti 500 x 500 (Formati [Iprom], 2008). Velikost video oglasa je s priporočili IAB omejena na 1,2 megabajta. Upoštevati se mora prijazno nalaganje oglasa, kar pomeni, da se vsebina glasa lahko začne nalagati šele potem, ko se je vsebina strani že naložila. Predvajanje oglasa se po tem priporočilu lahko zgodi šele, ko

se je oglas v celoti naložil na uporabnikov računalnik (Standards, Guidelines & Best Practices, 2008).

Oglasi z bogato predstavitveno vsebino (angl. *rich media ad*) – To so oglasi s katerimi lahko uporabnik spleta sodeluje in so izdelani v eni od spletnih tehnologij. Lahko vključujejo tudi zvok, sliko in animacije. Izdelani so v različnih spletnih tehnologijah, kot so Java, JavaScript, Flash itd. Oglasi z bogato predstavitveno vsebino se pojavljajo v obliki celostranskih ali lebdečih oglasov, raznih pravokotnikov, pa tudi v obliki pasic (Standards, Guidelines & Best Practices, 2008).

1.4 Načini spletnega oglaševanja

Organizacija IAB navaja več načinov spletnega oglaševanja (Internet Advertising Revenue Report 2007, 2008, str. 13):

Prikazovalno oglaševanje (ang. display advertising) je zelo razširjeno in ga uporablja večina komercialnih spletnih mest. Pri takem načinu oglaševanja oglaševalec plačuje bodisi podjetju, ki je lastnik spletne strani, ali podjetju, ki skrbi za oglaševanje na tej spletni strani, za prostor, kjer se prikazujejo njegovi oglasi. Oglasi so lahko v eni izmed pojavnih oblik, ki so bile predstavljene v poglavju 1.3.

Ustvarjanje povpraševanja (angl. *lead generation*) je ena izmed prvih oblik spletnega oglaševanja. Podjetja se z lastniki spletnih mest dogovorijo, da jim v zameno za določen znesek preusmerijo uporabnika na njihove spletne strani. Ta način oglaševanja se obnese predvsem takrat, ko se podjetje in spletno mesto ukvarjata s sorodno dejavnostjo. Če se njuni dejavnosti preveč razlikujeta, lahko pride do denarno spodbujenega ustvarjanja povpraševanja (angl. *incentive*), kar je največkrat nekoristno, saj obiskovalci niso prišli na strani podjetja, ki oglašuje, zaradi lastnih interesov.

Prodajni oglasi *(angl. classifieds)* so namenjeni oglaševanju prostih delovnih mest, avtomobilov, dražb, nepremičnin itd. Oglaševalec plača podjetju, ki take oglase gosti na svoji spletni strani, praviloma v enkratnem znesku za oglas.

Sponzorstvo (angl. *sponsorship*) predstavlja poljubno oglasno vsebino, ki jo gosti spletna stran in se navezuje na podjetje, ki stran oziroma dejavnost sponzorira.

Plačano vključevanje (angl. *paid inclusion*) zagotavlja, da bo oglaševalčev spletni naslov indeksiran s strani spletnega iskalnika. S tem načinom ne vplivamo na uvrstitev v iskalne rezultate, saj je v tem primeru spletni naslov oglaševalca prikazan med rezultati iskanja na podlagi običajnih algoritmov spletnega iskalnika.

Zakup iskalnih nizov (angl. *paid listings*) je način oglaševanja, ko oglaševalec plača spletnemu iskalniku, dase uporabniku, ko vnese določeni iskalni niz, na vrhu ali ob strani izpiše njegov tekstovni oglas. Primer takega načina oglaševanja so Google AdWords.

Vsebinsko iskanje (angl. *contextual search*) niza oglase na spletne strani na podlagi vsebine. Lahko so znotraj teksta v obliki spletnih povezav na posameznih besedah ali pa jim je namenjen določen prostor. Večinoma so v tekstovni obliki in se vsebinsko navezujejo na podjetje, ki oglašuje.

Poleg zgoraj omenjenih načinov je v okviru spletnega oglaševanja ključnega pomena tudi optimizacija spletnih strani (angl. *search engine optimisation* – SEO). To je proces urejanja in organiziranja vsebine in meta oznak spletne strani oziroma spletnega mesta, s čimer dosežemo boljše uvrstitve v spletnih iskalnikih. Za visoko uvrstitev v spletnih iskalnikih je pomembna tudi velika količina pravilno naslovljenih povezav, ki kažejo na našo stran z drugih spletnih strani. Optimizacija spletnih strani za iskalnike je ena ključnih aktivnosti spletnega oglaševanja. Lahko jo izvajamo specifično za določene iskalnike, kot so lokalni, iskalniki ali panožno usmerjeni iskalniki, ki jim pravimo tudi vertikalni.

1.5 Cenovni modeli (angl. *pricing models*)

V spletnem oglaševanju poznamo različne modele, s katerimi oglaševalec plačuje za opravljene storitve spletnega oglaševanja. Razlikujejo se po tem, kako se zaračunavajo stroški prikazanih oglasov.

Večina oglasnega prostora v Sloveniji se proda po ceni na prikaz (CNP), pri katerem se oglaševalcu obračuna vsak prikaz oglasa, oziroma po hibridnem modelu, kjer se uporablja kombinacija modelov CNP in CNK. Model, ki je bolj priljubljen med oglaševalci in manj med založniki, je model zakupa po ceni na klik (CNK), pri katerem se obračuna vsak klik uporabnika na oglas (Skrt, 2009).

Cena na prikaz CNP (angl. *cost per impression CPM*) - Ne plača se za vsak posamezni prikaz temveč, na tisoč, zato je v angleški inačici kratice črka »m«. Ta predstavlja izraz »mille«, ki v rimskih številkah pomeni tisoč.

Cena na klik CNK (angl. *cost per click CPC*) **ali plačilo na klik** (angl. *pay per klick*) - Oglaševalec v tem modelu plača samo takrat, ko uporabnik spleta klikne na prikazan oglas. Če se oglas samo prikaže in do klika uporabnika ne pride, se cena ne obračuna. Ta sistem je po svetu najbolj priljubljen, saj učinkovito izenači zahteve oglaševalcev in ponudnikov oglasnega prostora (Internet Advertising Revenue Report 2007, 2008). Zaradi njegove priljubljenosti in razširjenosti je tudi najbolj izpostavljem zlorabam. Plačilni model CNK je osnova, ki omogoča ustvarjanje lažnih klikov in nepravično izkoriščanje udeležencev spletnega oglaševanja.

Cena na ogled, cena na obisk CNO (angl. *cost per view, cost per visitor CPV*) - Ta model plačevanja oglasov je povsem podoben CNK-modelu. Razlikujeta se le po tem, da pri CNK-modelu oglaševalec plača ne glede ns to, ali je uporabniku uspelo priti do oglaševalčeve spletne strani, v primeru CNO pa je za plačilo oglasa obisk spletne strani oglaševalca nujen.

Cena na dejanje CND (angl. *cost per action CPA*) - Pri modelu CND oglaševalec plača samo za tiste oglase, ki so spodbudili uporabnika k določenemu dejanju, po katerem se cena oglasa zaračuna. Dejanje mora biti vnaprej dogovorjeno, predstavlja pa ga lahko nakup izdelka, izpolnitev obrazca, registracija itd. Tudi Google je uporabljal tak način plačevanja oglasov, vendar ga je iz programa AdSense izključil leta 2008 (Glossary [MarketingTerms], 2008).

Obstajajo še drugi plačilni modeli, ki se ne uporabljajo tako pogosto. **Cena na zanimanje** (angl. *cost per engagement*) predstavlja model, ko oglaševalec ne plača, ko se oglas prikaže in na kratko predstavi vsebino, ampak šele ko uporabnik namensko klikne nanj in požene celotno predstavitev oglasa, ki lahko traja tudi nekaj minut. Tak model je vpeljal spletni portal VideoEgg marca 2008 (VideoEgg Tries 'Cost per Engagement' [AdWeek], 2008). Model **cene na pridobitev CNP** (angl. *cost per aquisition CPA*) je zelo podoben modelu SND. Razlika je ta, da se za strošek pri CNP šteje le, ko se uporabnik spleta neposredno po oglasu odloči za nakup izdelka ali storitve. CNP lahko uvrstimo tudi kot podvrsto CND.

1.6 Potek izdelave oglaševalske akcije na spletu

Pogoj, da podjetje lahko prične oglaševati na spletu, je izdelano in urejeno spletno mesto, na katerega bodo oglasi preusmerjali uporabnike spleta. Brez lastne spletne strani bo podjetje samo z oglasi na spletu zelo težko uveljavljalo svojo prisotnost. Namen spletnih mest je ponuditi informacije o izdelkih ali storitvah, ponuditi možnost spletnega naročila ali nakupa ter utrjevanje blagovne znamke. Če bo podjetje privabilo na spletno stran več ciljnega občinstva, bo imelo od spletne strani večjo finančno korist.

Ko ima podjetje dokončno izdelano spletno mesto, ki je objavljeno na svetovnem spletu, moramo poskrbeti, da bo vidno v največjih iskalnikih. Začne lahko z brezplačnim vpisom v slovenske spletne iskalnike Najdi.si, Matkurja.com, Slowwwenia.com, kar bo podjetju omogočilo vidnost tudi v pomembnejših svetovnih iskalnikih. Naslednji korak predstavlja optimizacijo spletnih strani za iskalnike, tako da bo spletno mesto postavljeno čim više v zadetkih posameznih iskalnikov.

Podjetje, ki ima urejeno mesto in je ustrezno uvrščeno v spletne iskalnike, lahko prične s pripravo spletnih oglasov in z zakupom oglasnega prostora na ustreznih spletnih mestih. Zakup oglasnega prostora lahko opravi neposredno pri lastniku spletnega mesta ali pa to prepusti eni izmed spletnih oglaševalskih mrež. Httpool in Iprom sta trenutno največji oglaševalski mreži v Sloveniji. Spletno oglaševanje preko oglaševalskih mrež je boljša izbira za večino podjetij, ki želijo učinkovito oglaševati na spletu z relativno majhnimi stroški. Oglaševalske mreže poleg načrtovanja, vodenja in merjenja uspešnosti oglaševalskih akcij nudijo tudi zakup oglasnega prostora na vseh spletnih mestih v svoji mreži. Tako podjetje prihrani veliko dragocenega časa in denarja, saj lahko preko enega posrednika zakupi oglasni

prostor pri večjem številu izbranih medijev hkrati, zaradi česar mu ni potrebno sklepati pogodb z vsakim posebej (Cerar, 2004, str. 21).

Pri zakupu oglasnega prostora se mora podjetje odločiti, po kakšnem cenovnem modelu bo oglasni prostor najelo. Včasih so oglaševalci na spletu plačali fiksni znesek za gostovanje spletnega oglasa za določen čas. Danes prevladujejo cenovni modeli, ki sem jih podrobno že opisal v predhodnem poglavju. Iztopata modela CNK ali CNP. Najdemo tudi njuno kominacijo. Cena na prikaz je velikokrat odvisna tudi od velikosti oglasa in njegove postavitve na spletni strani oziroma spletnem mestu. Najbolj pogoste postavitve glede na spletno stran so na vrhu, na desni strani ali na dnu. Glede na spletno mesto pa so lahko na prvi strani ali na podstraneh.

Če se podjetje odloči za oglaševanje z uporabo cenovnega modela CNK, mora vzpostaviti ustrezno analitiko, ki bo omogočala odkrivanje lažnih klikov. Svojim zaposlenim, odgovornim za učinkovitost investicij v oglaševnaje, mora omogočiti ustrezno izobraževanje na temo lažnih klikov. Odvisno od velikosti vložkov v spletno oglaševanje se mora odločiti, ali bo uporabljalo enega izmed plačljivih izdelkov za odkrivanje lažnih klikov, ki jih ponujajo zunanji izvajalci, ali pa se bo odločilo za lastne rešitve.

Ko je oglas izdelan in ko se je podjetje dogovorilo za način in stroške prikazovanja pri ponudnikih spletnih oglasnih prostorov, lahko prične z oglaševanjem. Oglase mora ves čas pojavljanja na spletu spremljati, meriti učinke in ustrezno ukrepati, če želi, da bo njegova oglaševalska akcija v celoti uspešna. Spletno oglaševanje ima pred ostalimi oblikami oglaševanja prednost, da lahko oglaševalsko akcijo s pomočjo oglaševalskih orodij spremljamo v realnem času in oglaševanje po potrebi optimiziramo. To pomeni, da lahko oglaševalec spremlja učinkovitost posameznih oglasnih mest in spletnih oglasov pred, med in po akciji ter v času poteka akcije z njimi upravlja: menjava spletne pasice in oglasna mesta, upravlja z dosegom in frekvenco oglasnih sporočil.

S tovrstnimi orodji lahko podjetje izmeri tudi učinkovitost oglasov, s katerimi oglašuje. Kazalniku, ki ponazarja število klikov na oglas v razmerju z njegovimi prikazi, pravimo stopnja klikov. Z njim lahko ugotovimo kolikšna je priljubljenost oglasa med uporabniki.

Število klikov in s tem tudi stopnja klikov sta odvisna predvsem od kreativnosti in vsebine oglasa ter od primernosti oglaševane vsebine glede na občinstvo. Večjo odzivnost in s tem stopnjo klikov podjetje doseže tako, da oglas postavlja na spletna mesta, kjer je vsebina povezana z izdelkom oziroma storitvijo, ki jo podjetje oglašuje. Na primer: če podjetje želi oglaševati računalniško opremo, je priporočljivo, da svoje oglase postavi na spletna mesta, ki so povezana z informacijskimi tehnologijami (Cerar, 2004, str. 20).

V zadnji fazi oglaševalske akcije sledi izdelava poročil o opravljenem oglaševanju. Podjetja, ki oglašujejo na spletu, lahko z nekoliko zmogljivejšimi orodji za ugotavljanje uspešnosti oglaševalskih akcij pridejo po koncu le-teh do podatkov o tem, kako so se premikali, koliko časa so se zadrževali in kaj so klikali posamezni uporabniki, ki so med drugim kliknili tudi na

njihov oglas. Če ima podjetje na svoji spletni strani vzpostavljeno tudi spletno naročanje izdelkov oziroma storitev, si lahko izračuna, koliko naročil je bilo izvedenih preko spletnega oglasa in kolikšen je povprečen strošek oglaševanja za posamezna naročila.

V diplomski nalogi sem do te točke predstavil spletno oglaševanje z njegovimi pojavnimi oblikami in cenovnimi modeli, ki so osnova za razumevanje problematike, ki jo predstavljajo lažni kliki na spletne oglase. V nadaljevanju bom predstavil natančnejši opis modela CNK in predstavil najbolj razširjena oglaševalska programa, temelječa na njem. Na podlagi le-teh bom nato predstavil osnovne pogoje in razloge, ki so povzročili ustvarjanje lažnih klikov.

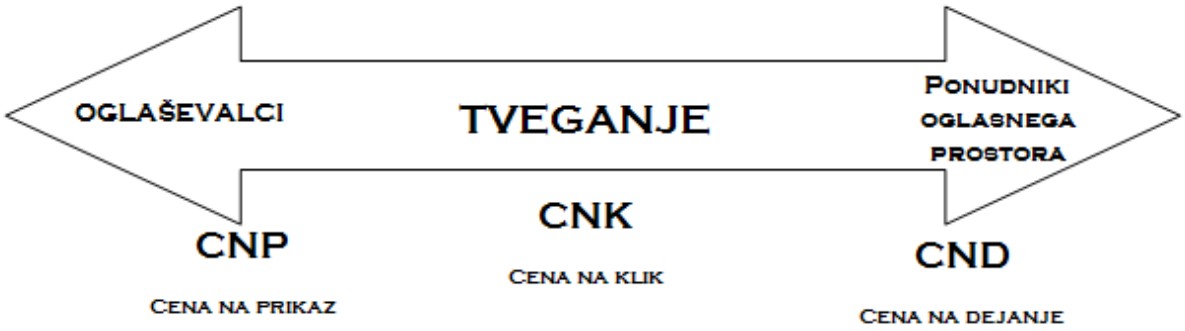
2 LAŽNI KLIKI

Veliko število udeležencev, umetno povečanje zaslužka, relativno enostavne možnosti zlorab, globalna razpršenost in anonimnost so ključni dejavniki, ki povzročajo masovno ustvarjanje lažnih klikov v spletnem oglaševanju. Delež velikih vložkov podjetij, ki se ustrezno ne zavarujejo pred tovrstnimi zlorabami, vsako leto konča na računih zlonamernežev, ki se na ta način okoriščajo. Kljub velikim prizadevanjem največjih oglaševalskih mrež, da bi izkoreninile oziroma ustrezno ugotavljale lažne klike, je cenovni model CNK še vedno močno izpostavljen tovrstnim zlorabam.

V preteklosti se je za plačevanje oglaševalskih akcij v spletnem oglaševanju večinoma uporabljal plačilni model cena na prikaz (CNP). Največkrat je merjen v ceni na tisoč prikazov (angl. *CPM – Cost per mille*). Izhaja iz tradicionalnega načina oglaševanja, kjer se stroški oglaševanja izračunajo na podlagi števila potencialnih ogledov oglasa v izbranem mediju.

Slika 8 prikazuje delitev tveganja med udeleženci v spletnem oglaševanju glede na izbrani plačilni model. Ponudniki oglasnega prostora na spletu najraje uporabljajo plačilni model CNP, saj so njihovi prihodki neodvisni od uspešnosti posameznega oglasa. Kljub temu so spletni iskalniki v spletnem oglaševanju razširili plačilni model CNK. Ta je bolj naklonjen oglaševalcem kot CNP, saj plačajo le za tiste oglase, na katere so uporabniki spleta kliknili. S tem modelom izenačimo tveganje med oglaševalci in ponudniki oglasnega prostora. Lastniki spletnih mest tvegajo s tem, ko so plačani le takrat, ko je uporabnik dejansko kliknil na oglas, kar pa je zanje vsekakor boljše kot model CND. Oglaševalci pri modelu CNK tvegajo, saj plačajo za vsak klik na oglas, ne glede na to, ali so imeli od uporabnika, ki je na oglas kliknil, kakšne koristi ali ne. Priljubljenost cenovnega modela CNK izvira iz delitve tveganja med ponudniki oglasnega prostora in oglaševalci (Mitchell & Linden, 2006, str. 2).

Slika 8: Delitev tveganja med udeleženci spletnega oglaševanja glede na plačilne modele



Vir: S. Mitchell & J. Linden, Click Fraud: What is it and how we make it go away?, 2006, str. 2.

V nadaljevanju bom predstavil oglaševalska programa znanega podjetja s področja spletnega oglaševanja, na podlagi katerih bom predstavil ključni problematiki lažnih klikov.

Za razširitev plačilnega modela CNK je še posebej zaslužno podjetje Google z oglaševalskima programoma AdWords in AdSense.

AdWords je oglaševalski program za podjetja, ki želijo oglaševati na spletu. Preko dražbe zakupijo določen iskalni niz in si tako zagotovijo, da se poleg rezultatov iskanja prikazuje njihov oglas ali pa se le-ta, če je dovolj zanimiv, prikazuje na spletnih mestih različnih ponudnikov oglasnega prostora, ki so povezani v Googlovo oglaševalsko mrežo. Takemu načinu oglaševanja pravimo tudi zakup iskalnih nizov (angl. *paid listings*). Ker uporabnika zanima tematika, poleg katere se oglasi prikazujejo, je zelo verjetno, da bo kliknil na tak oglas.

Na Slika 9 je prikazano delovanje dveh trenutno največjih oglaševalskih mrež. Oglasi vstopijo v oglaševalsko mrežo preko aplikacij Google AdWords in Yahoo! Search Marketing in se nato nizajo na različne spletne strani, ki so v lasti oglaševalske mreže, pridruženih članov ali ponudnikov oglasnega prostora, prijavljenih v oglaševalsko mrežo preko programov Google AdSense in Yahoo! Publisher Network.

Oglaševalski program AdSense temelji na mreži spletnih mest, kjer podjetje Google nastopa kot posrednik. Program je namenjen lastnikom spletnih mest, ki želijo ustvariti zaslužek v zameno za prikazovanje oglasov na svojih spletnih straneh. Oglasi, ki se servirajo na takih spletnih mestih, so bili predhodno vključeni v program AdWords.

Slika 9: Shema oglaševanja preko oglaševalski mrež

Vir: S. Mitchell & J. Linden, Click Fraud: What is it and how we make it go away?, 2006, str. 6.

Google nato samodejno pregleduje vsebino spletnih mest, ki so prijavljena v program AdSense kot ponudniki oglaševalskega prostora (angl. publishers), in niza oglase na tista spletna mesta, kjer je vsebina tesno poveznana z zakupljenimi ključnimi besedami podjetja, ki oglašuje. Vsakič, ko kdo klikne na tak oglas, se del prihodkov iz oglaševanja dodeli ponudniku oglaševalskega prostora, del pa ostane podjetju Google, ki nastopa v tem primeru kot oglaševalska mreža.

Na podlagi primera oglaševalskih programov podjetja Google lahko ločimo dva načina generiranja lažnih klikov: lažni kliki konkurentov in lažni kliki ponudnikov oglasnega prostora.

Lažni kliki konkurentov

Lažni kliki konkurentov podjetja, ki oglašuje preko spleta, ne nastanejo zaradi denarne koristi, ampak da bi škodili svojim konkurentom. Pri tem načinu generiranja klikov mora biti oškodovano podjetje prijavljeno na enega izmed oglaševalskih programov, ki uporablja

plačilni model CNK (npr. AdWords). Konkurent podjetja pozna logiko delovanja oglaševalskega programa in ve, da vsak klik na oglas predstavlja za podjetje, ki oglašuje, določen strošek. Oškodovanemu podjetju taki kliki na oglas ne prinašajo koristi, saj za njimi ni realnega zanimanja za vsebino oglasa. Konkurenti lahko klikajo na oglase ročno ali pa s pomočjo naprednih aplikacij (Stricchiola, 2008).

Lažni kliki ponudnikov oglasnega prostora

S pomočjo generiranja lažnih klikov se lahko okoristijo tudi ponudniki oglasnega prostora. Lastniki spletnih mest, ki so vključena v programe oglaševalskih mrež, kot je AdSense, lahko z generiranjem lažnih klikov na oglase, ki se nahajajo na njihovih spletnih straneh, umetno povečajo svoj prihodek. Tudi v tem primeru poznamo bolj in manj napredne načine generiranja lažnih klikov. Večina ponudnikov oglasnega prostora, ki s pomočjo generiranja lažnih klikov povečuje svoj prihodek, je prehodnih in pogosto menja lokacijo in vrsto spletnih mest (Soubusta, 2008, str. 136-137).

Za primer prepovedanih dejanj ponudnikov oglasnega prostora navajam izsek iz pogojev poslovanja oglaševalske mreže ToBoAds (Pogoji in pravila [ToBoAds], 2009).

»Kot ponudnik oglasnega prostora pod nobeni pogoji ne smete (niti ne smete tega dovoliti ali na to nagovarjati katerokoli tretjo osebo):

1. *posredno ali neposredno ustvarjati Promet na katerikoli Oglas preko kakršnihkoli avtomatičnih, prikritih, sleparskih, ali drugih nepravilnih sredstev, kar brez izjeme vključuje ponavljajoče osebni klike, uporabo robotov ali druge programske opreme, ki avtomatizira Promet;*

2. *popravljati, filtrirati ali spreminjati vrstni red informacij, ki so prikazane v kateremkoli Oglasu, ali izbrisati, zakriti, popačiti katerikoli Oglas v kakršnemkoli smislu;*

3. *uokviriti, minimizirati, odstraniti ali drugače preprečiti celoten in popoln prikaz katerekoli Oglaševane strani, ki je dostopna končnemu uporabniki preko klika na katerikoli del Oglasa;*

4. *preusmeriti končnega uporabnika stran od katerekoli Oglaševane strani ali ga preusmeriti preko neke druge strani na Oglaševano stran; vsi kliki opravljeni na Oglas morajo končnega uporabnika direktno, brez kakršnihkoli vmesnih postankov pripeljati na Oglaševano stran;*

5. *prikazovati kakršnihkoli Oglasov na straneh z napako, kar brez izjeme vključuje 404 Document not found. Prav tako ne smete prikazovati Oglasov na kakršnikoli strani z registracijo, ali na strani kjer se zahvaljujete uporabniku za registracijo, v katerikoli elektronski pošti, pogovorni (“chat”) strani, ali pa na strani, ki vsebuje pornografske, rasno nestrpne, nasilne, žaljive ali nelegalne vsebine;*

6. *posredno ali neposredno dostopati, zaganjati, in/ali aktivirati Oglasov, ali kako drugače vključevati Oglase v kakršnokoli aplikacijo ali spletno stran, ki ni Vaša Stran; to lahko storite samo v obsegu, ki je dovoljen s tem Dogovorom;*

7. *v kakršnikoli obliki pridobivati in shranjevati informacije, pridobljene s katerimkoli Oglasom;*

8. *delovati na kakršenkoli način, ki ni v skladu s PU ali sodelovati v katerikoli akciji ali praksi, ki bi metala slabo luč na Tobonet ali bi kako drugače omalovaževala, razvrednotila ali škodovala Tobonetovemu ugledu. Strinjate se, da kakršnokoli kršenje teh pravil, lahko vodi do pravnega pregona proti Vam, vključujoč tudi takojšnjo izključitev iz ToboAds.«*

Za oglaševalce na spletu lažni kliki predstavljajo velik problem. Oglaševalci ugotavljajo, da se oglaševalske mreže ne trudijo dovolj, da bi take klike preprečile. Gre za nespoštovanje dogovora med oglaševalci in oglaševalskimi mrežami, ki se v pogodbi večinoma strinjajo, da bodo poravnale vse morebitne stroške, ki izvirajo iz lažnih klikov na oglase. Oglaševalci so takoj, ko so opazili, da so bili bremenjeni tudi za lažne klike, pričeli tožiti oglaševalske mreže (Google's Adwords - Advertising Practices [Lawyers and Settlements], 2010).

2.1 Pomembnost odkrivanja lažnih klikov

Leta 2005 je skupni prihodek iz spletnega oglaševanja znašal 12,5 milijarde dolarjev, leta 2006 je porasel za 35 odstotkov, na vrednost 16,9 milijarde dolarjev (Internet Advertising Revenue Report 2007, 2008, str. 6). Leta 2007 so v prvem četrtletju prihodki iz oglaševanja znašali 4,9 milijarde dolarjev, leta 2008 pa 5,9 milijarde dolarjev. Čeprav so ti zneski videti zelo majhni v primerjavi s tistimi iz televizijskega oglaševanja in oglaševanja v tiskanih medijih, ki leta 2006 znašali 48,3 in 46,6 milijarde dolarjev, je trend rasti očitno večji pri spletnem oglaševanju. Rast prihodkov iz televizijskega oglaševanja je leta 2006 znašala 5,3 odstotka, rast oglaševanja v tiskanih medijih pa ni presegala niti 2 odstotkov (Soubusta, 2008, str. 138).

V organizaciji Click Forensics ugotavljajo, da je približno vsak šesti klik lažen, čeprav ne morejo z zagotovostjo trditi, kakšno je njihovo realno število (Industry Click Fraud Rate Hovers at 16 Percent for Third Quarter, 2009). Lažni kliki niso le dodaten strošek za podjetja, ki oglašujejo preko spleta, temveč lahko po najbolj pesimističnih napovedih povzročijo kolaps celotnega sistema spletnega oglaševanja. Samo klikanje na spletne oglase ni zapleteno opravilo in prinaša zlonamernežem razmeroma velike prihodke. Zato se je število posameznikov in skupin, ki se okoriščajo z oglaševalskimi programi, v zadnjih nekaj letih strmo povečalo. Velik delež lažnih klikov v oglaševalskih programih, ki uporabljajo plačilni model CNK, lahko preobremeni podjetja z oglaševalskimi stroški, ki se ne prenesejo v porast prodaje oglaševanega izdelka ali storitve. Podjetja lahko začnejo umikati neprofitabilne naložbe v spletno oglaševanje in tožijo oglaševalske mreže za nastalo škodo. Oglaševalske

mreže tako izgubijo stranke in njihov prihodek se prične zmanjševati (Kitts, LeBlanc, Meech & Laxminarayan, 2008).

Pomembnosti odkrivanja lažnih klikov se zavedajo tudi v največjem spletnem oglaševalskem podjetju Google. Nedavno so omogočili raziskovalcu Aleksandru Tuzhilinu, profesorju z univerze v New Yorku, da si pobliže ogleda sistem za odkrivanje lažnih klikov v podjetju in oceni, ali si Google dovolj prizadeva take klike odkriti. Google se je za tako potezo odločil zato, ker je veliko podjetij, ki oglašujejo preko njihovih programov, večkrat podvomilo v njihov sistem za odkrivanje lažnih klikov. Nekateri primeri so se končali tudi s tožbo (Tuzhilin, 2008).

Tudi v podjetju Yahoo! se po navedbah Patricka Giordanija, odgovornega za analize in upravljanje s tveganji, trudijo vzpostaviti najmodernejši sistem za preprečevanje lažnih klikov. Pri njih so se strokovnjaki s področja spletnih aplikacij odločili za večnivojsko strukturo sistema za odkrivanje lažnih klikov. Kot posebnost navaja, da veliko komunicirajo z oglaševalci, s katerimi si izmenjuje informacije (Stricchiola, 2008).

2.2 Število lažnih klikov

Zaradi težav, ki so povezane z odkrivanjem, je določanje stopnje lažnih klikov v celotni spletni oglaševalski panogi zelo zahtevno. Podjetje Click Forensics združuje več kot 4.500 oglaševalskih mrež in podjetij, ki na njih oglašujejo, v Mrežo lažnih klikov (*angl. Click fraud network*). Na podlagi podatkov, zbranih iz mreže, se izmeri indeks lažnih klikov (*angl. Click fraud index*). Mreža lažnih klikov zbira statistične podatke panoge spletnega oglaševanja in vključuje tako majhna kot velika podjetja, ki oglašujejo na spletu. Podatki o lažnih klikih se zbirajo in predstavljajo na četrtletni ravni. Storitev pregleduje podatke tako na spletnih straneh oglaševalskih mrež kot tudi na spletnih straneh podjetij, ki oglašujejo na spletu.

Rezultati statistike za tretje četrtletje leta 2008 prikazujejo, da je v celotni spletni oglaševalski panogi stopnja lažnih klikov 16-odstotna. Stopnja se je znižala glede na drugo četrtletje 2008 in tretje četrtletje 2007, ko je v obeh primerih znašala 16,2 odstotka. Povprečna stopnja lažnih klikov na oglase, ki uporabljajo plačilni model CNK in se prikazujejo preko programov oglaševalskih mrež, kot sta Googlov AdSense in Yahoojev Publisher Network, je bila v tretjem četrtletju 2008 27,1 odstotka. Tudi v tem primeru se je stopnja lažnih klikov znižala v primerjavi z enakim obdobjem lani, ko je znašala 28,1 odstotka. Lažni kliki, ustvarjeni s pomočjo klikbotov, so predstavljali 27,6 odstotka vseh lažnih klikov v tretjem četrtletju 2008. Največji delež lažnih klikov je v tem obdobju prihajal iz Rusije (4,9 odstotka), Francije (4,8 odstotka), in Velike Britanije (3,5 odstotka).

Tom Cuthbert, predsednik uprave podjetja Click Forensics, pravi, da se v zadnjih obdobjih stopnja lažnih klikov giblje okoli 16 odstotkov. Počasi se zmanjšuje, kar pripisuje vedno večjemu zavedanju oglaševalcev in proaktivnim vključevanjem v odkrivanje lažnih klikov, preden ti prizadenejo njihove oglaševalske akcije. Kljub temu pa se število lažnih klikov s

strani klikbotov povečuje in predstavlja trenutno eno največjih nevarnosti za celotno spletno oglaševalsko panogo. Tom Cuthbert poziva vse oglaševalce in oglaševalske mreže, naj posvetijo čim več truda opazovanju in odkrivanju delovanja klikbotov (Industry Click Fraud Rate Hovers at 16 Percent for Third Quarter [Click Forensics], 2008).

3 USTVARJANJE LAŽNIH KLIKOV

Kot je značilno za ostale zlorabe informacijske tehnologije, se tudi lažni kliki pojavljajo v različnih stopnjah. Najpreprostejše ustvarjanje lažnih klikov je tako, da konkurent klika na oglase svojega konkurenta in mu s tem zmanjšuje razpoložljivi vložek za oglaševanje. Tak način ustvarjanja lažnih klikov je danes mogoče odkriti s preprostimi algoritmi, s kateremi so opremljeni sodobni oglaševalski programi. Aplikacije, ki strežejo z oglasi na spletnih straneh imajo vgrajene filtre, ki tovrstne klike izločijo in poskrbijo, da oglaševalec zanje ne bo bremenjen.

Izurjeni goljufi izdelujejo posebne avtomatizirane aplikacije za generiranje lažnih klikov ali pa uporabljajo skupine ljudi, ki klikajo na oglase, ne da bi se zavedali, da s tem komu škodijo. V primeru podjetja iz ZDA je bila za veliko količino lažnih klikov na oglase posameznih spletnih mest odgovorna večja skupina ljudi v Indiji, ki so za majhno plačilo klikali na oglase (Vidyasagar, 2004).

Plačilo za branje (angl. paid to read)

Lastniki spletnih mest, ki ponujajo nagrade za klikanje na oglase in izpolnjevanje prijavnih obrazcev, so eden večjih generatorjev lažnih klikov v spletnem oglaševanju. Taki programi ponujajo svojim članom točke, denar ali podobne nagrade v zameno za klikanje na oglase in pregledovanje spletnih strani. Člani so umetno spodbujeni, da klikajo na oglase in berejo vsebino spletnih strani oglaševalcev, s čimer ustvarjajo večinoma nezaželene klike. Večina se jih niti ne zaveda, kaj pomeni ustvarjati lažne klike in kaj njihovo početje predstavlja za celotno spletno oglaševalsko panogo.

Klikboti (angl. clickbots)

Klikboti so avtomatizirane aplikacije, ki jih lahko vsak posameznih prenese preko interneta. Programirane so tako, da ustvarjajo lažne klike, ki se v aplikacijah za spremljanje in ugotavljanje lažnega prometa prikazujejo kot veljavni. S posebnimi tehnikami prikrivajo izvirni IP-naslov (angl. *Internet protocol address*) računalnika, na katerem gostujejo, in previdno klikajo na oglase v različnih časovnih intervalih z namenom, da oponašajo človeku podobno ravnanje. IP-naslov je kombinacija številk, ki je dodeljena vsakemu računalniku povezanemu v internet. Veliko klikbotov za prikrivanje svojega izvirnega IP-naslova uporablja naključne namestniške strežnike (angl. *proxy*) po vsem svetu, ki jim omogočajo simulacijo naravnega spletnega prometa. Lokacije takih klikbotov težko odkrijemo in prepoznamo njihovo prisotnost v oglaševalskih programih. Nekateri tipi tovrstnih aplikacij se

v obliki prikrite aplikacije, imenovane trojanski klikbot (angl. trojan clickbots), ali virusa namestijo na računalnik uporabnika spleta brez njegove vednosti. Prikriti klikboti se aktivirajo med uporabo spletnega brskalnika in sprožajo nevidne klike po oglasih. Razmnožujejo se preko raznih kanalov, kot so internet, zgoščenke, diskete, FTP-strežnikov ali preko trenutno zelo aktualnih omrežij za izmenjavo datotek med uporabniki spleta (angl. peer-to-peer network). Odkriti jih je skoraj nemogoče, saj se skrivajo za resničnimi uporabniki spleta in njihovimi računalniki. Omrežja računalnikov, okuženih s trojanskimi klikboti, imenujemo botneti (*angl. botnets*).

V nadaljevanju sem si za predstavitev delovanja aplikacije klikbot izbral popularno rešitev za samodejno ustvarjanje lažnih klikov Clicking Agent. Na spletu je razširjena zaradi enostavne namestitve in uporabe. Možno jo je brezplačno pridobiti tudi v preizkusni različici. Po navedbah avtorja aplikacije je bilo do leta 2006 nelegalno prodanih okoli 5000 licenc, kar je v omenjenem obdobju prinašalo okoli 10.000 dolarjev letno.

3.1 Predstavitev klikbota

Clicking Agent je klikbot aplikacija, ki omogoča samodejno klikanje na spletne oglase. Aplikacijo je razvil ruski programer iz Sibirije in jo namenil tistim, ki bi radi namerno škodovali podjetjem, ki oglašujejo na spletu. Kljub temu, večina ljudi uporablja aplikacijo Clicking agent za umetno povečevanje klikov na oglase na lastnih spletnih mestih. Aplikacijo je mogoče kupiti preko spleta za 100 ameriških dolarjev.

Aplikacija je zasnovana tako, da generira klike na oglase izbranega spletnega mesta. S pomočjo namestniških strežnikov prikaže, kot, da kliki izvirajo z različnih koncev sveta, čeprav se največkrat nahaja na istem strežniku kot spletno mesto. Ob ustrezni parameterizaciji aplikacije lahko kliki delujejo realni tudi večjim oglaševalskim mrežam kot sta Googlov AdSense in Yahoo! Publisher Network.

3.1.1 Uporaba aplikacije Clicking Agent

Aplikacijo prenesemo s spleta in jo namestimo na računalnik, ki ima dostop do spleta. Če jo namestimo na računalnik, ki je v splet povezan preko usmerjevalnika, moramo na njem ustrezno nastaviti posredovanje prometa. To storimo tako, da odpremo na usmerjevalniku ustrezna vrata in promet preusmerimo na računalnik, kjer gostuje aplikacija Clicking Agent.

Naslednji korak v postopku je parameterizacija aplikacije. Najprej moramo pripraviti seznam namestniških strežnikov, ki bodo služili za lažno prikazovanje izvora generiranih klikov na oglase. Sezname obstoječih namestniških strežnikov lahko najdemo na različnih spletnih naslovih, kot sta checkedproxylist.com in cgiproxylist.com. Aplikaciji lahko nastavimo frekvence po posameznih časovnih intervalih v dnevu. Tako se kliki iz posameznih časovnih pasov generirajo v ustreznih intervalih, ko naj bi bilo v tistem območju največ internetnega

prometa. Izbiramo lahko, kateri spletni brskalniki in kako pogosto se bodo pojavljali v generiranih klikih, kot tudi katere regionalne nastavitve bodo uporabljane. Aplikacija omogoča tudi avtomatično izpolnjevanje obrazcev na spletni strani podjetja, ki oglašuje. V tem primeru moramo nastaviti ustrezne kombinacije imen polj in obrazcev, ki jih bo aplikacija izpolnila in poslala v primeru, da naleti nanje. V nadaljevanju moramo definirati, na katerih spletnih mestih želimo, da aplikacija generira lažne klike in kako pogosto (Clicking Agent - A curse or myth for advertisers? [Cvanci], 2008).

3.1.2 Pogoji za uspešno generiranje lažnih klikov

Za prikrivanje izvora generiranih klikov je najpomembneje, da aplikaciji vnesemo dober seznam namestniških strežnikov. Aplikacija sicer omogoča dodajanje in posodabljanje teh seznamov vendar se neprestano spreminjajo in lahko se zgodi, da v enem dnevu namestniški strežnik izgine ali pa se znajde na seznamu nevarnih (*angl. blacklist*). Promet s takih strežnikov je takoj označen kot sumljiv in je v večini oglaševalskih programov samodejno izločen. Izkušenejši goljufi uporabljajo posebne spletne aplikacije, ki neprestano iščejo nove namestniške strežnike in njihove IP-naslove. To je za današnje računalnike zelo zahtevna operacija zaradi ogromnega števila kombinacij IP-naslovov, iz katerih lahko poiščemo veljavne naslove uporabnih namestniških strežnikov. Za izračun bi povprečen računalnik potreboval 300 let. Zato večina goljufov išče samo v določeni državi ali regiji, kjer je znano, da obstaja več javno dostopnih namestniških strežnikov. To pa omogoča standardnim tehnikam za odkrivanje lažnih klikov veliko lažje delo, saj so države s spornimi namestniškimi strežniki, kot sta Kitajska in Rusija, znane tudi oglaševalskim mrežam. (Livingstone, 2004).

Odkrivanje lažnih klikov, ki jih generira aplikacija Clicking Agent, je zelo težka naloga, če se omejimo na pregledovanje glav HTTP-zahtevkov, kjer se nahajajo podatki o računalniku, ki sproža klike. Program zna namreč oponašati obnašanje večine obstoječih spletnih brskalnikov, operacijskih sistemov in jezikov ter ustrezno procesira piškotke in JavaScript. Večina teh nastavitev je prilagodljivih, tako da jih lahko uporabnik aplikacije nastavi na podlagi trenutnih spletnih statistik.

Aplikacija je delujoča in ob pravilni parameterizaciji lahko zelo škodljiva za oglaševalce. Njena slabost je, da ji moramo večkrat dnevno posredovati seznam IP-naslovov aktivnih namestniških strežnikov, kar ni lahka naloga. Upraba ustrezno parameterizirane aplikacije za rahlo povečanje prometa spletnemu mestu, ki uživa razmeroma velik dnevni obisk, je lahko zelo uspešna in nudi lastnikom spletnih mest dodaten zaslužek. Lastnik spletnega mesta, ki ima malo prometa in bo samo z uporabo te aplikacije umetno povečeval promet, bo na večini oglaševalskih mrež hitro odkrit. Mreže mu v takem primeru zaprejo račun in preprečijo nadalno uporabo a oglaševalskega programa (Clicking Agent - A curse or myth for advertisers? [Cvanci], 2008).

3.2 Botnet

Omrežje računalnikov, na katerih so nameščene trojanske klikbot aplikacije, imenujemo botnet. Taka omrežja omogočajo tistim, ki jih nadzirajo, možnost porazdelitve klikov na tisoče ali celo milijone IP-naslovov po vsem svetu. V tem primeru ni potrebno iskati veljavnih namestniških strežnikov, da bi prikrili dejanski izvor klikov, saj vsi izvirajo iz obstoječih računalnikov, povezanih v splet.

3.2.1 Prevzemanje oblasti nad računalnikom

Ciljni računalnik lahko prevzamemo s pomočjo izkoriščanja varnostnih poman,kljivosti v posameznih aplikacijah na njem. Programe, ki izkoriščajo take pomanjkljivosti imenujemo izkoriščevalci (angl. *exploit*). Napadalci jih sami napišejo ali pa uporabijo obstoječe, ki so dostopni preko spleta. Večina uporablja tehniko prekoračenje pomnilnika (angl. *buffer overflow*). Do prekoračitve pride, ko program ali proces poiskuša shraniti na dodeljeni pomnilniški prostor več podatkov, kot jih je ta pripravljen sprejeti. Ker si pomnilniški prostori sledijo v zaporedju, lahko tako prepišemo veljavne podatke v naslednjem pomnilniškem prostoru z vrinjeno programsko kodo, ki izvede zlonamerne operacije. Ko se napadalec odloči, katero pomanjkljivost sistema bo izkoristil, prične z iskanjem možnih žrtev na spletu. Izbrani žrtvi vrine zlonamerno programsko kodo, s katero pridobi nadzor nad računalnikom. Take računalnike napadalec upravlja s pomočjo aplikacije, za centraliziran nadzor botneta.

3.2.2 Nadziranje botneta

Največkrat se za upravljanje botneta uporabi protokol internet relay chat (IRC). Sestavljen je iz enega ali več strežnikov, ki komunicirajo z odjemalci s pomočjo sporočil. Tako lahko upravljalec botneta nadzira okužene računalnike in preko njihovih IP-naslovov generira lažne klike na oglase na svojih spletnih straneh.

Botnet lahko upravljamo tudi preko spletnega vmesnika, na katerega so povezani okuženi računalniki. Slabost tega načina je, da mora odjemalec neprestano zahtevati posodobitve od upravljalca, medtem ko pri upravljanju preko IRC to ni potrebno. Spletni vmesniki povzročijo praviloma tudi več spletnega prometa med samim delovanjem, kar lahko poveča možnosti odkritja botneta. Praviloma mora upravljalski center za botnet uporabljati pogosto uporabljani protokol in preko njega povzročati čim manj prometa, da ostane v spletu neviden (Soubusta, 2008, str. 138-139).

3.3 Uporaba JavaScripta za generiranje lažnih klikov

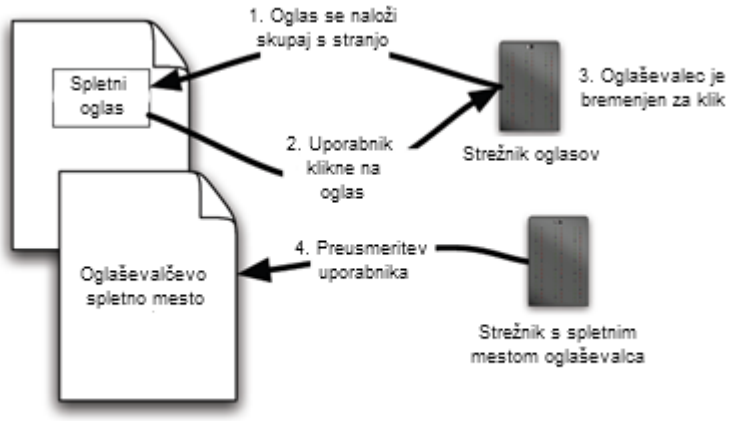
Lastniki spletnih mest, ki ponujajo oglasni prostor se lahko za generiranje lažnih klikov poslužujejo različnih tehnik. Ena izmed njih je uporaba zlonamerne kode JavaScript, ki se izvaja na uporabnikovem brskalniku. To je možno le, če uporabnikov brskalnik omogoča

njeno izvajanje. Oglaševalske mreže, ki oglase strežejo na spletne strani, to delajo s pomočjo manjših programskih funkcij v JavaScriptu, ki jih lastniki spletnih mest vključijo na spletne strani. Če ima uporabnik Javascript v brskalniku onemogočen, se mu taki oglasi ne prikazujejo.

3.3.1 Prikaz oglasov z uporabo JavaScript funkcij

Za razumevanje takega napada je potrebno najprej poznati delovanje tehnologije in logike, ki omogoča centralizirano posredovanje oglasov na različna spletna mesta. Tak način streženja oglasov je prikazan na Slika 10: Streženje oglasov na spletne strani. Sodobne oglaševalske mreže strežejo oglase na spletna mesta tako, da posredujejo lastniku spletnega mesta funkcijo, napisano v JavaScriptu, ki jo le ta doda na spletne strani. Ta programska koda se izvede v uporabnikovem brskalniku vsakič, ko zahteva tako spletno stran. Koda sproži prenos oglasov s strežnika oglaševalske mreže, ki skrbi za posredovanje ustreznih oglasov, na spletno stran. Prenos oglasov sproži prepisovanje okvirja, kjer se je nahaja koda JavaScript, s HTML-kodo, ki omogoča prikaz oglasov na spletni strani. Kadar uporabnik spleta klikne na tak oglas, se razen tega, da uporabnika preusmeri na ustrezno spletno stran oglaševalca, sproži tudi klic do strežnika oglasov, ki lahko na podlagi prejetih parametrov bremeni oglaševalca za znesek oglasa in lastniku spletnega mesta dodeli ustrezno provizijo (Soubusta, 2008, str. 139).

Slika 10: Streženje oglasov na spletne strani



Vir: M. Gandhi, M. Jakobsson, & J. Ratkiewicz, Badvertisments: Stealthy Click-Fraud with Unwitting Accessories, 2006, str. 6.

Napad z uporabo JavaScripta, ki ga opisujem spodaj, je mogoče izvesti le, če oglaševalska mreža streže oglase z ranljivo kodo JavaScript. Večina oglaševalskih mrež že uporablja varno tehniko prikazovanja oglasov. To sem preveril in ugotovil, da tako Googlov AdSense kot tudi slovenski oglaševalski mreži ToBoAds podjetja Httpool in AdPartner uporabljajo varen način streženja z oglasi.

Nezavarovana koda JavaScript uporablja funkcijo print_ads(), s katero zapiše oglase neposredno na trenutno spletno stran. V primeru varne kode JavaScript funkcija print_ads najprej zapiše HTML značko <iframe>, v kateri se oglasi izpišejo s pomočjo dodatno definirane funkcije. To omogoča brskalnikom, da zavarujejo vsebino <iframe> značke pred ostalimi funkcijami JavaScript na spletni strani.

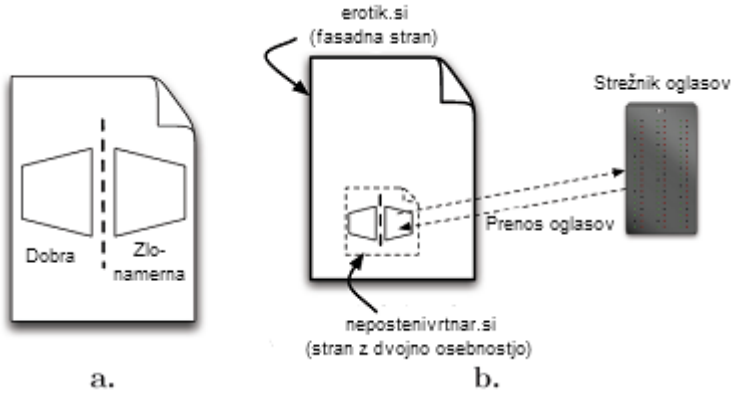
3.3.2 Stran z dvojno osebnostjo in fasadna stran

Z uporabo zlonamerne kode JavaScript lahko spreminjamo običajne oglase v zlonamerne. Uspešen zlonameren oglas je tisti, ki omogoča nevidno ustvarjenje klikov na oglase, ko spletno stran obiščejo uporabniki, in ostane neopažen, ko spletno stran obišče spletni agent oglaševalske mreže. Spletni agent ali pajek je aplikacija, ki v izvirni različici služi oglaševalskim mrežam in spletnim iskalnikom za indeksiranje spletnih strani. Takega pretvarjanja pa ne moremo doseči le s prikazovanjem zlonamernih oglasov vsem, ki se ne predstavijo kot spletni agent oglaševalske mreže. Znano je, da oglaševalske mreže opravljajo tudi naključne preglede strani, pri katerih se ne predstavijo z lastnim nazivom. Poleg umetnega generiranja klikov lahko zlonameren lastnik spletnega mesta s pomočjo omenjene tehnike priredi tudi vsebino spletnih strani, na primer s pornografskimi vsebinami in s tem poveča promet na strani.

Na tem mestu se srečamo z novima pojmoma: fasadna stran in stran z dvojno osebnostjo. Fasadna stran prikazuje samo vsebino brez zlonamernih oglasov. Njena vsebina so lahko pornografske slike ali posnetki, ki so v večini primerov prepovedani s strani oglaševalske mreže, ki določa vsebine na spletnih straneh, na katerih so oglasi. Fasadna stran deluje v povezavi s stranjo z dvojno osebnostjo, katere funkcija je spreminjanje izgleda iz dobrega v zlonamernega na podlagi tipa obiskovalca. Ko stran obišče uporabnik spleta, se prikaže v zlonamernem izgledu, kadar pa jo obišče spletni agent oglaševalske mreže, se prikaže kot dobra oziroma veljavna. V nadaljevanju predpostavljam, da obstajata dve spletni mesti, in sicer www.erotik.si, ki vsebuje fasadno stran, in www.nepostenivrtnar.si, ki vsebuje stran z dvojno osebnostjo.

V prvem delu Slika 11 je pod točko a predstavljena stran z dvojno osebnostjo, ki prikazuje uporabnikom spleta zlonamerne oglase. Ko tako stran pregleda spletni agent, se prikaže kot dobra. Točka b prikazuje stran z dvojno osebnostjo, vključeno v fasadno stran. Fasadna stran prikazuje nedovoljeno vsebino in skriva zlonamerno plat strani z dvojno osebnostjo, ki v ozadju samodejno sproža klike na oglase (Gandhi et al., 2006, str. 5-6).

Slika 11: Prikaz logike delovanja fasadne strani in strani z dvojno osebnostjo.



Vir: M. Gandhi, M. Jakobsson, & J. Ratkiewicz, Badvertisments: Stealthy Click-Fraud with Unwitting Accessories, 2006, str. 6.

V primerjavi z izvirnimi oglasi so zlonamerni dopolnjeni s kodo JavaScript in sprožijo na spletni strani spremembe, ki spremenijo normalen proces prikazovanja, klikanja in preusmerjanja spletnih oglasov. Potem ko se izvede koda JavaScript oglaševalske mreže in prepiše stran tako, da ta vsebuje oglase, koda JavaScript zlonamernega oglasa pregleda HTML-kodo prikazanih oglasov in iz nje izdela seznam vseh povezav. Nato zlonamerna koda spremeni stran tako, da ta vsebuje značko <iframe>, ki omogoča spletnemu brskalniku hkrati prikazovati vsebino dveh različnih spletnih strani. Značka <iframe> v tem primeru omogoča, da se znotraj nje naloži vsebina spletne strani podjetja, ki oglašuje v posameznem oglasu. To se zgodi vsakič, ko se samodejno zgenerira klik na oglas. Uporabnik tega ne opazi, saj je lahko celotna stran z dvojno osebnostjo, ki gostuje zlonamerne oglase, vključena v fasadno stran s pomočjo skrite značke <iframe>.

Slika 12: Delovanje zlonamernih oglasov

Vir: M. Gandhi, M. Jakobsson, & J. Ratkiewicz, Badvertisments: Stealthy Click-Fraud with Unwitting Accessories, 2006, str. 7.

Fasadna stran služi za to, da s pomočjo pornografskih vsebin privabi čim več obiskovalcev. Ta sistem omogoča samodejno ustvarjanje lažnih klikov, ki navidezno prihajajo s pletnega mesta www.nepostenivrtnar.si vsakič ko uporabnik spleta obišče spletno stran na www.erotik.si. Proces delovanja zlonamernih oglasov je prikazan na Slika 12.

3.3.3 Prikrivanje sledi pred spletnimi pajki

Opisana tehnika deluje s pomočjo vrinjene kode JavaScript, ki zna pregledovati in spreminjati veljavno kodo, s katero oglaševalska mreža prikaže oglase na spletno stran. Zlonamerno kodo pa lahko s posebno tehniko programiranja tako popačimo, da ne moremo ugotoviti, kako se obnaša, dokler je ne izvedemo. To lastnikom spletnih strani omogoča, da skrijejo vsebino zlonamernih oglasov pred spletnimi agenti, ki iščejo vzorce programske kode, ki so znani in povezani z ustvarjanjem lažnih klikov. Ena od metod popačenja uporablja funkcijo eval(), ki omogoča, da iz zapletenih konstant, zapisanih v obliki niza podatkov, izluščimo in izvedemo veljavno kodo JavaScript. Slika 13 prikazuje, kako lahko uporabimo tehniko popačenja z uporabo funkcije eval. V obeh primerih, ko jo poženemo, funkcija izpiše števila od ena do deset.

Slika 13: Popačenje kode JavaScript

(a)
```
for( i = 1; i <= 10; i++ ) {
   document.write( i );
}
```

(b)
```
code = "f@o"+"#r(i@"+"#="+1+";@"+"i#<=1%0"+";i"
       +"+@#+){@"+"d#oc"+"%um#"+"en%t."+"@w#r"
       +"i#te"+"(@i + \"<b" + "r>\");}";
eval(code.replace(/[@#%]/g, ""));
```

Vir: M. Gandhi, M. Jakobsson, & J. Ratkiewicz, Badvertisments: Stealthy Click-Fraud with Unwitting Accessories, 2006, str. 7.

Pri tem načinu prevare je pomembno, kako bomo skrili zlonamerno obnašanje strani z dvojno osebnostjo. Oglaševalske mreže najpogosteje uporabljajo pregledovanje strani (angl. *spidering*) s pomočjo spletnih agentov ali pajkov (angl. *spiders*). Pajki lahko uporabljajo dva načina pregledovanja strani: običajno pregledovanje (angl. *standard (forward) spidering*) in povratno pregledovanje (angl. *reverse spidering*).

Pri običajnem pregledovanju spletnih strani bo pajek prišel na stran www.erotik.si, se pretvarjal, da je navaden uporabnik, in bo kot tak tudi obravnavan. Posebnost večine pajkov je, da ne pregledujejo kode Javascript saj je ta praviloma namenjena interakciji z uporabnikom in ne za generiranje teksta. Če pajek pregleduje tudi ukaze JavaScript, se uporabi ena od tehnik popačenja. V tem primeru se fasadno stran na www.erotik.si napiše tako, da prične z zlonamernim delovanjem šele čez nekaj trenutkov, ko se izvede koda

JavaScript. V tem primeru pajek ne opazi prikritega delovanja strani z dvojno osebnostjo v ozadju in odide s spletnega mesta.

Povratno pregledovanje strani poteka v nasprotni smeri kot običajno. Povratni pajek sledi povezavam, ki so jih sprožili kliki na oglase. Lastniki spletnih mest lahko uvedejo pravilo, da strežejo zlonamerne oglase samo obiskovalcem, ki so prišli na stran prvič. Tako bi povezava, ki jo je uporabil pajek, že imela šifro obstoječega obiskovalca in bi se spletna stran z dvojno osebnostjo na www.nepostenivrtnar.si, od koder je klik izviral, prikazala v dobri luči.

Lastnik spletnega mesta www.nepostenivrtnar.si lahko uporabi dodatna pravila kdaj, se bo stran z dvojno osebnostjo na njegovem spletnem mestu obnašala zlonamerno. Uvajanje dodatnih pravil oteži odkrivanje, saj bo moral spletni pajek zadostiti določenim pravilom, da bo lahko odkril zlonamerne oglase. To seveda tudi zmanjša promet, ki ga lastnik spletnega mesta lahko izkoristi za ustvarjanje lažnih klikov, vendar je na dolgi rok to dobra odločitev, saj bo zmanjšal možnost, da ga odkrijejo. Primer uvedbe posebnih pravil je, da prikažemo zlonamerne oglase samo takrat, ko uporabnik na fasadni strani prenese določeno število posnetkov ali slik (Gandhi et al., 2006, str. 11).

3.3.4 Možnost hitrega zaslužka

To je način zlorabe spletnega oglaševanja, s katerim si lahko zlonamerni lastniki spletnih mest povečujejo prihodek. V primerjavi s krajo identitete, ki je trenutno ena najbolj razširjenih tehnik za krajo in zlorabo podatkov na spletu, je ta tehnika manj kompleksna in jo lahko izvede skoraj vsak zlonameren lastnik spletnega mesta, ki je prijavljen v eno od ranljivih oglaševalskih mrež. Monetizacija zlorabe je takojšnja, saj je denar, ki ga pridobimo s tem načinom goljufanja, prenesen neposredno na naš račun. Prikazana tehnika je izvedljiva le preko oglaševalskih mrež, ki strežejo oglase z ranljivo kodo.

4 ODKRIVANJE LAŽNIH KLIKOV

Ustvarjanje lažnih klikov v spletnem oglaševanju je velik problem, ki se ga je treba lotiti sistematično. Največja težava vseh podjetij, ki se ukvarjajo z njihovim odkrivanjem, je določiti, kaj je lažni klik. Premalo je svetovnih standardov, ki bi opredeljevali lažne klike in tako omogočili njihovo lažje odkrivanje in poenotili poročanje. Prav pri poročanju oglaševalskih mrež podjetjem, ki oglašujejo, nastopijo težave, saj ima ponavadi vsaka stran svoj pogled na lažne klike. S tem bi se izognili mnogim tožbam na tem področju. Spletna oglaševalska panoga se ne more zanesti na to, da vsaka oglaševalska mreža pripravlja svoje specifikacije o lažnih klikih. Organizacije, kot sta SEMPO in IAB, imajo komisije, ki se ukvarjajo z definiranjem tovrstnih standardov. V najboljšem primeru bodo te hiše izdale standard, s katerim se bodo vse oglaševalske mreže in oglaševalci strinjali (Mitchell & Linden, 2006, str. 11).

Glede na to, da ne poznamo standardov, ki bi definirali lažne klike, se morajo podjetja, ki so zadolžena za njihovo odkrivanje znajti in uporabljati svoje definicije.

Lažni kliki (angl. *click fraud*) nastanejo v plačilnem modelu CNK, ko oseba, avtomatizirana skripta ali računalniški program oponaša dejanja uporabnika spleta, ki klika na spletne oglase, z namenom, da se pri tem okoristi.

Večina oglaševalskih mrež ne uporablja izraza lažni, temveč neveljavni kliki. Izraz neveljavni se je uveljavil, ker oglaševalske mreže ne morejo v vseh primerih jasno določiti, ali je bil klik zlonameren ali ne.

Google - V Googlu določajo neveljavne klike na podlagi lastne definicije, ki pravi, da so neveljavni kliki vsi tisti, ki so pridobljeni iz naslova plačilnega modela CNK, ki so umetno ustvarjeni s pomočjo človeških ali tehnoloških virov z edinim namenom bremenitve klika in kjer ni nikakršne možnosti, da bo prišlo do nakupa oglaševanega izdelka ali storitve (Mordkovich & Mordkovich, 2007).

Yahoo! - V podjetju Yahoo! se s spletnim oglaševanjem ukvarja oddelek za oglaševanje preko iskalnikov (angl. *search marketing*), kjer pojmujejo kot lažne vse neupravičene klike, ki izvirajo bodisi iz avtomatiziranih programov bodisi iz človekovih dejanj (Click fraud FAQ [Yahoo!], 2009).

Microsoft - V Microsoftovem adCentru definirajo kot neveljaven tisti klik, ki so mu pripisali lastnosti, značilne za uporabniške napake, zlonamerna dejanja ali podobne tipe neveljavnih aktivnosti (Mordkovich & Mordkovich, 2007).

Ask.com - Neveljavni so kliki, ustvarjeni s pomočjo robotov, sistemov ali programov, ki niso imeli namena obiskati spletne strani oglaševalca (Mordkovich & Mordkovich, 2007).

Vse definicije v grobem vključujejo splošna dejstva, ki se jih da v določeni meri konkretizirati.

- Lažni kliki so lahko ustvarjeni s pomočjo človeških dejanj ali tehnoloških pripomočkov in vključujejo različne vrste zlonamernih programov, kot so skripte in klikboti.

- Ko preverjamo veljavnost klika, moramo razumeti s kakšnim namenom je uporabnik kliknil na oglas. Na podlagi tega določimo, ali je obstajal namen nakupa izdelka ali pa je bil klik ustvarjen samo zato, da bi se nekdo okoristil.

- Klike lahko ugotovimo tudi pred nastankom z odkritjem zlonamernih programov, vključenih v spletne strani, kjer se nizajo oglasi. Oglaševalske mreže imajo v pristopnih pogodbah za ponudnike oglasnega prostora definirano, da je uporaba takih programov strogo prepovedana. Odkritje krištelja pomeni ukinitev njegovega računa pri oglaševalski mreži.

4.1 Odkrivanje lažnih klikov s strani oglaševalskih mrež

Omenil sem že oglaševalske mreže in njihovo spopadanje z definicijami lažnih klikov, ki jim služijo za uvajanje teorije v prakso ter odkrivanje lažnih klikov. Navkljub njihovemu trudu pa je vsaj zaenkrat tudi teoretično vse lažne klike nemogoče odkriti.

Oglaševalske mreže uvajajo nove metode odkrivanja lažnih klikov, da bi zadovoljile zahteve oglaševalcev. V podjetjih Google in Yahoo!, kjer upravljajo z dvema največjima oglaševalskima mrežama, so priznali, da so težave z lažnimi kliki nevarnost ne le za njihov poslovni model, temveč tudi za vsesplošen uspeh obeh podjetij.

Google odkrivanju lažnih klikov posveča več pozornosti kakor Yahoo!. Posvetili so se globinskemu iskanju surovih podatkov o klikih, da bi našli vzorce lažnih klikov. Oglaševalske mreže čedalje bolj uvajajo namenske sisteme za odkrivanje lažnih klikov, ki se nenehno posodabljajo, tako da so kos tudi najnovejšim zvijačam zlonamernih udeležencev v spletnem oglaševanju (Mordkovich & Mordkovich, 2007).

Oglaševalci želijo videti konkretne rešitve združenj podjetij pod okriljem agencije IAB, saj imajo le-ta na voljo vedno več koristnih informacij o lažnih klikih tudi iz strani mreže Click Network Group, s katerimi bi lahko prišla do uporabnih predlogov in rešitev.

Oglaševalske mreže javnosti redko razkrijejo koliko denarja vrnejo oglaševalcem, ko ti odkrijejo sumljive klike na svoje oglase. V podjetju Google oglaševalcu, ki dokaže obstoj sumljivih klikov, denar vedno vrnejo (How will Google credit my account for invalid clicks? [Google AdWords], 2009). Posledica ugotovljenih lažnih klikov se odraža tudi na računih ponudnikov oglasnega prostora, kjer so bili ugotovljeni. Prihodek lastnikov spletnih mest se v teh primerih zmanjša. Google je leta 2004 posegel po pravni poti, saj je tožil podjetje Auctions Expert International, ki je po trditvah upravljalcev oglasnega programa AdSense namerno klikalo na oglase na njihovem spletnem mestu z namenom, da se okoristi (Google lawsuit Auction Expert International [WebOptimiser], 2009).

Kljub trditvam oglaševalskih mrež, da vselej vračajo stroške za prijavljene lažne klike in odkrivajo metode za njihovo samodejno izločanje, veliko oglaševalcev meni, da se ne trudijo dovolj, da bi težavo rešili. Veliko jih je obupanih, ker jim ne uspe zbrati dovolj dokazov, da bi prepričali oglaševalske mreže o zlonamernih aktivnostih na svojih oglasih. Mrežam je sicer v interesu, da so oglaševalci zadovoljni, vendar je v ozadju tudi njihov poslovni interes. Če bi bili bolj popustljivi, do oglaševalcev, bi se pojavili tudi oglaševalci, ki bi si skušali umetno znižati stroške oglaševanja.

Večje oglaševalske mreže imajo večinoma lastno programsko opremo za odkrivanje lažnih klikov. V podjetju Yahoo! razvijajo in dopolnjujejo tak sistem že od leta 1998 in danes pregleduje okoli petdeset različnih kriterijev: od zelo preprostihn kot so IP-naslov, piškotki ali informacije o uporabnikovem brskalniku, do bolj kompleksnih, ki odkrivajo vzorce zlonamernega obnašanja spletnih mest. Ko je izpolnjeno določeno število kriterijev, se klik označi kot neveljaven in se ne uvrsti na seznam tistih, ki bremenijo oglaševalca (Mordkovich & Mordkovich, 2007).

Oglaševalske mreže pozivajo oglaševalce, da naj poročajo o sumljivih aktivnostih na svojih oglasih, saj lahko z ustreznimi utemeljitvami dobijo denar za lažne klike povrnjen. Če so njihovi zahtevki zavrnjeni, morajo vztrajati in prepričati oglaševalske mreže, da so se zgodile zlonamerne aktivnosti na njihovih oglasih. Z vztrajanjem pri pošiljanju zahtevkov za povračilo stroškov povečajo možnost, da zadevo obravnaval analitik in morda odkril, da ima oglaševalec prav.

Nekatere oglaševalske mreže imajo formalizirane sisteme za odkrivanje lažnih klikov. Primera takih sistemov sta programski opremi TrueLead podjetja LookSmart in ValidClick podjetja Kowabunga. Večina oglaševalskih mrež operira z neformaliziranimi sistemi za odkrivanje lažnih klikov, ki so plod lastnega razvoja. Nekatere se odločijo za združitev zunanje programske opreme, ki jo po potrebi dopolnjujejo z lastnim sistemom za odkrivanje lažnih klikov. Vse oglaševalske mreže nudijo možnost povračila stroškov za lažne klike na oglase, če so ustrezno utemeljeni.

4.2 Kaj lahko storijo oglaševalci

V vsaki zgodbi o lažnih klikih je na koncu oškodovano podjetje, ki je plačalo za prikaz oglasov. Podjetja, ki oglašujejo prek spleta samo zato, ker je trenutno v modi ali pa zato, ker se zgledujejo po konkurentih, nimajo zadostnih znanj o spletnem oglaševanju in o tem kako uspešno izdelati oglaševalsko akcijo, ki bi povečala prodajo izdelkov ali storitev. Primanjkuje ustrezne literature, ki bi uslužbence v podjetjih informirala o posebnostih spletnega oglaševanja. Prevečkrat se ga enači z oglaševanjem preko tradicionalnih medijev, kot so radio, časopisi in televizija.

O lažnih klikih, ki so ena pomembnejših tem, povezanih spletnim oglaševanjem, je gradiva še manj in oglaševalci težko sledijo novim vrstam zlorab. Razlogov je več. Oglaševanje preko spleta s pomočjo plačilnega modela CNK je zaživelo v zadnjih petih letih in z njim so se pojavile tudi zlorabe. Tudi če je literatura na voljo, jo oglaševalci težko razumejo, ker se ne spoznajo na spletne tehnologije in in ne vedo, kako ukrepati, da bi ugotavljali zlorabe na svojih oglasih.

Lažni kliki v spletnem oglaševanju s plačilnim modelom CNK so dejstvo, ki se mu ne more izogniti noben oglaševalec in se je z njimi potrebno spopasti na ustrezen način. V predhodnih poglavjih sem opisal vrste napadov in načine odkrivanja, ki jih uporabljajo oglaševalske mreže. Te imajo dostikrat premalo podatkov o celotnem procesu klikanja skozi oglase (*angl. klick trough*). Zato morajo oglaševalci na strežnikih, kjer gostujejo njihove spletne strani, uporabiti orodja za odkrivanje lažnih klikov. Najbolje je, da proizvajalci teh orodij niso vključeni v oglaševalski proces (*angl. third-party tools*).

Veliko oglaševalskih mrež nima ustrezno vzpostavljene politike in aplikacij za odkrivanje lažnih klikov. Nekatere odkrijejo le delček lažnih klikov in tako oglaševalcem, ki želijo pošteno plačevati za svoje oglase, ne preostane drugega kot da se lotijo odkrivanja sami.

Velika težava je količina časa, ki ga lahko oglaševalci porabijo za analize in organiziranje dokazov o lažnih klikih, ki jih kasneje lahko pokažejo oglaševalskim mrežam, da jim

povrnejo stroške. Pogosto je čas, vložen v odkrivanje zlorab posamezne oglaševalske akcije, več vreden kot stroški, ki jih lahko dobimo povrnjene s takimi dokazi. Kadri, ki se ukvarjajo s spletnim oglaševanjem v podjetju, morajo biti ustrezno izobraženi in vzpostavljeni morajo biti pravilni postopki ugotavljanja lažnih klikov. Oglaševalci se stroškov, povezanih z izobraževanjem kadrov, ustrašijo in o klikih ne poročajo oziroma se sami sebe prepričajo, da se na njihovih oglasih take stvari ne dogajajo. Tega so najbolj veseli goljufi, ki se z lažnimi kliki na njihove oglase okoriščajo.

Specifično načrtovana orodja za odkrivanje sledi lažnih klikov od proizvajalcev, ki niso vpleteni v oglaševalski proces, lahko oglaševalcu pomagajo analizirati arhivske datoteke prometa preko oglasov in odkriti, ali je bil morda žrtev lažnih klikov. Taka orodja lahko tudi zvišajo njihovo kredibilnost pri oglaševalski mreži in tako povečajo možnost, da bo dobil za reklamirane klike denar res povrnjen.

4.2.1 Orodja za odkrivanje lažnih klikov zunanjih izvajalcev

Oglaševalci se zavedajo problematike lažnih klikov in potrebujejo orodja za njihovo odkrivanje. To priložnost so iskoristili zunanji izvajalci in ponudili tako programsko opremo na tržišče.

Zunanji izvajalci razvijajo programsko opremo, namenjeno odkrivanju lažnih klikov, ki jo oglaševalci lahko implementirajo na svoja spletna mesta. Oglaševalci si s temi orodji pomagajo pri nadziranju prometa, ki je prispel na njihova spletna mesta preko spletnih oglasov, in na podlagi pridobljenih informacij izdelujejo poročila, s katerimi lahko zahtevajo vračilo stroškov pri oglaševalskih mrežah.

Orodja zunanjih izvajalcev temeljijo na pregledovanju prometa, ki je preko oglasov prišel na spletno mesto oglaševalca. Z njimi lahko pregledujejo aktivnosti uporabnika tudi potem, ko je že kliknil na oglas. Oglaševalske mreže so pri tem zelo omejene, saj večina oglaševalcev ne želi namestiti programske opreme oglaševalske mreže, ki bi zbirala podatke o prometu na njihovih spletnih mestih. V takih primerih se lahko oglaševalske mreže zanesejo le na podatke, ki so jih zbrale do takrat, ko se je zgodil klik na oglas, in posledično preusmeritev na spletno stran oglaševalca.

Obratno pa velja, da programska oprema zunanjih izvajalcev nima nadzora nad prometom, ki se dogaja na spletnih mestih, kjer oglas gostuje. Odkrivanje lažnih klikov na podlagi aktivnosti, ki se dogajajo za tem, ko uporabnik klikne na oglas, je učinkovito za veliko vrst lažnih klikov, vendar se slabo izkaže pri naprednejših tehnikah, ki zlorabljajo uporabnike spleta za generiranje lažnih klikov. Slabše zasnovana programska oprema zunanjih izvajalcev bi lahko predpostavljala, da so kliki veljavni, ker izvirajo iz resničnih uporabnikov spleta, čeprav v resnici ti uporabniki niti ne vedo, da so se lažni kliki generirali med njihovim brskanjem po straneh.

Uporaba orodij za odkrivanje lažnih klikov zunanjih izvajalcev ni problematična z vidika implementacije na spletno mesto in oglase. Oglaševalec mora poskrbeti za namestitev manjše komponente JavaScript na tiste spletne strani, na katere so povezani oglasi, in dodati sledilne

značke (angl. *tracking tags*) v spletne naslove, ki se pojavljajo v spletnih povezavah na samih oglasih.

Ko oglaševalec uspešno implementira orodje za odkrivanje lažnih klikov, lahko pregleduje promet uporabnikov na svojem spletnem mestu v poročilih. Orodja za odkrivanje lažnih klikov, ki jih oglaševalec implementira na svoje spletno mesto, ne pregledujejo vsega prometa, ampak samo tistega, ki izvira iz oglaševalskih mrež, na katerih gostujejo njegovi oglasi. To pa pomeni, da morajo oglaševalci, ki oglašujejo pri več oglaševalskih mrežah, orodjem za odkrivanje lažnih klikov to prijaviti, da jim omogočijo ustrezno analiziranje prometa.

Omenjena orodja zbirajo različne podatke, ki jih je moč razbrati iz aktivnosti uporabnika na spletu. Primer poročila takih podatkov je prikazan na Slika 14. S pomočjo teh podatkov se izdelajo kriteriji, ki določajo veljavnost posameznih klikov (Click Fraud Detective FAQ [Click Fraud Detective], 2009).

IP naslov - Poznamo statične (angl. *static IP*) in dinamične (angl. *dynamic IP*) IP-naslove. Pri dinamičnih se določenemu računalniku skozi čas IP-naslov spreminja. V tem primeru orodja za odkrivanje lažnih klikov prepoznajo računalnike s spreminjajočimi IP-naslovi in jih posledično pravilno obravnavajo.

Slika 14: Primer poročila o lažnih klikih

Total Unique IDs: 100 Total Unique IDs with more than 1 occurrence: 5
Total PPC Clicks: 109 PPC Clicks with more than 1 occurrence: 14

PPC Clicks with more than 1 occurrence(s)

Click Time	Unique ID	IP Address	PPC Used	Referrer	Country	Domain	ISP	Keywords	Landing Page
2006-11-07 10:28:52	23f75210-864f-4a67-89b8-b07c53751565	129.42.161.	google	google.com	UNITED STATES	IBM.COM	IBM CORPORATION	click fraud	http://www.whosclickingwho.com/?src=google&gclid=COvp1f3FtYqCFQ23WAodUTaUiw
2006-11-07 07:52:36	425fe332-7e5c-4dbd-9494-c54da8f510b1	193.63.247.	google	google.co.uk	UNITED KINGDOM	DA.MOD.UK	ROYAL MILITARY COLLEGE OF SCIENCE	click fraud	http://www.whosclickingwho.com/?src=google&gclid=CIPVvoejtYqCFTVYQgodLAIbiA
2006-11-07 07:52:09	425fe332-7e5c-4dbd-9494-c54da8f510b1	193.63.247.	google	google.co.uk	UNITED KINGDOM	DA.MOD.UK	ROYAL MILITARY COLLEGE OF SCIENCE	click fraud	http://www.whosclickingwho.com/?src=google&gclid=CO3pwvqjtYqCFSoMQgodFC3SiA
2006-10-30 12:07:41	8a3d9a35-b501-4abb-aafb-fbbfe71d6fb6	24.123.66.	google	google.com	UNITED STATES	RR.COM	ROAD RUNNER-COMMERCIAL	click fraud	http://www.whosclickingwho.com/?src=google&gclid=CNCVhZXNoYqCFUbAJAodxGAMLg

Vir: Sample Reports [WhosClickingWho?], 10.2.2009.

Uporabnikov agent (angl. *user agent*) - Skupek brskalnika in operacijskega sistema, ki sta bila uporabljena za tvorbo zahtevka za prikaz spletne strani.

Lokacija računalnika, ki je zahteval spletno stran - To je približna lokacija, omejena na regijo ali državo. S to informacijo si lahko pomagamo pri odkrivanju sumljivega prometa iz držav s povečanim deležem lažnih klikov.

Datum in čas prihoda uporabnika na spletno mesto oglaševalca - Podatek je pomemben za določanje pogostosti posameznih klikov na oglase v določenem intervalu.

Oglaševalska mreža - Oglaševalska mreža, preko katere je bil ustvarjen klik, ki je prinesel uporabnika na spletno mesto oglaševalca.

Ključne besede - Nekatera podjetja upravljajo poleg oglaševalskih mrež tudi spletne iskalnike. Če uporabnik spleta pride do oglasa preko spletnega iskalnika z določenim nizom ključnih besed, so te vljučene v povezavo, ki vodi do oglaševalca.

Edinstvena šifra (angl. *unique ID*) - Šifra označi posameznega obiskovalca spletnega mesta oglaševalca s šifro, vstavljeno v piškotek na uporabniškem brskalniku. Če uporabnik piškotek zavrne, se ustvari šifra seje na strežniku. Z identifikacijo posameznega uporabnika spleta lahko ločimo tudi med tistimi uporabniki, ki dostopajo preko namestniških strežnikov in di delijo isti IP-naslov.

Poizvedba IP-naslova - Poizvedba lahko poteka preko registra ARIN (American Registry of Internet Numbers), ki upravlja s storitvijo WHOIS. Ta omogoča prikaz podatkov, povezanih z IP-naslovom računalnika. S posamezno poizvedbo pridobimo podatke o naslovih, kontaktnih osebah ter nazivih operaterjev in podjetij, preko katerih je prišel promet do oglaševalčevega spletnega mesta.

Zgodovina IP-naslova - Zgodovina IP-naslova v celotnem prometu vseh spletnih mest, ki jih upravlja orodje za odkrivanje lažnih klikov. Tovrstne informacije omogočajo odkritje uporabnikov, ki klikajo na oglase enkrat ali dvakrat mesečno, vendar konstantno skozi celo leto.

4.2.2 Priporočila za oglaševalce

Oglaševalci, ki imajo vzpostavljen sistem za pregledovanje prometa in odkrivanje lažnih klikov na svojem spletnem mestu, lahko že sami veliko storijo in odkrijejo možne lažne klike, ki so jih morda spregledali v oglaševalskih mrežah. S pomočjo nekaterih sledi se lahko lažne klike hitro odkrije, za bolj prikrite je potrebno več poglobljenega preverjanja in raziskovanja. Oglasne mreže pregledujejo in odkrivajo lažne klike s pomočjo naprednih programskih rešitev. Nekatere nudijo tudi orodja za namestitev na spletno mesto oglaševalca, s katerimi se poveča uspešnost pri odkrivanju. Dobra praksa pravi, da je v vsakem primeru dobro imeti pri sebi možnost avtonomnega pregledovanja in odkrivanja lažnih klikov, bodisi s pregledovanjem dnevniških datotek na strežniku bodisi z uporabo namenske programske opreme za odkrivanje lažnih klikov zunanjega izvajalca.

V nadaljevanju bom podal nekaj priporočil, ki se jih je dobro držati pri spremljanju statistik oglaševalske akcije. Ne glede na to, ali bo oglaševalec s pregledovanjem prometa na svojem spletnem mestu odkril vzorce, ki so značilni za lažne klike, ali ne, je taka aktivnost dobrodošla, saj lahko ugotovi tudi druge pomanjkljivosti oglaševalske akcije, na podlagi katerih lahko kasneje opravi izboljšave in poveča ROI. S pregledovanjem naslednjih podatkov

lahko oglaševalec prepreči, da bi se na njegovem računu za spletno oglaševanje znašli tudi nezaželeni lažni kliki.

Nenadne spremembe - Če oglaševalec opazi, da je promet po določenih ključnih besedah, ki do tedaj niso bile posebej uspešne, porasel, naj prične s poizvedovanjem. Če oglaševalec sodeluje pri različnih oglaševalskih mrežah, lahko kot prvi korak loči promet in preveri, če se je povečanje zgodilo pri vseh ali samo pri določenem ponudniku oglaševalskih storitev. Na ta način lahko podrobneje pregleduje promet po posamezni oglaševalski mreži in ugotovi, ali se pri kateri izmed njih pojavljajo lažni kliki. Tak način omogoča lažje obvladovanje manjših delov statistik, iz katerih je bolj razvidno, ali se določen IP-naslov pojavlja večkrat. Prav tako kot porast prometa po posameznih oglaševalskih mrežah je lahko nevaren tudi porast celotnega prometa, če ni utemeljen s sezonskimi nihanji, trženjskimi potezami podjetja ali logično povezanimi dogodki, ki bi lahko nanj vplivali.

Padec kazalnikov uspešnosti - Če je vaša oglaševalska akcija uspešna in nenadoma opazite padec, lahko to pomeni, da ste žrtev napada. Porast števila lažnih klikov se odraža na ROI, saj se stroški z oglaševanjem povečujejo, medtem ko učinek oglaševalske akcije na oglaševani izdelek ali storitev ostaja nespremenjen.

Nenavadno veliko število klikov z istega IP-naslova - Čeprav je to najbolj očitna in lahko ugotovljiva oblika lažnih klikov, je še vedno veliko zlonamernežev, ki uporabljajo to metodo za izvedbo hitrih napadov. Izvedejo jih v obdobju praznikov, ko podjetja ne pregledujejo statistik Ko se zaposleni vrnejo na delo, lahko dobijo povsem izpraznjen račun za oglaševanje.

Veliko število obiskovalcev, ki hitro zapustijo spletno mesto - Veliko število obiskovalcev, ki so preko klika na oglas prišli na oglaševalčevo spletno mesto in ga takoj za tem zapustili, je tudi lahko znak lažnih klikov. Primerno je, da ima oglaševalec na spletnem mestu tako programsko opremo, ki zna slediti dejanjem uporabnika, in na podlagi tega določiti, ali je bil klik na oglas lažen ali ne. Anupam, Mayer, Nissim, Pinkas in Reiter (1999, str. 1097-1098) predlagajo uporabo metodologije, ki prepozna premike miške po spletnih straneh, značilne za resnične uporabnike spleta, in omogoča lažje odkrivanje aplikacij klikbot.

Povečano število klikov na pridruženih spletnih straneh (angl. affiliate websites) - Veliki spletni iskalniki, kot sta Google in Yahoo!, imajo dostikrat sklenjene pogodbe z manjšimi oglaševalskimi mrežami in iskalniki, preko katerih nizajo svoje oglase. Velike oglaševalske mreže omogočajo takim pridruženim podjetjem, da sama dodajajo spletna mesta v okviru lastnega omrežja, na katerem se prikazujejo oglasi oglaševalskih mrež, v katere so vključena. To pa v praksi pomeni manjšo stopnjo nadzora nad kakovostjo spletnih mest, prijavljenih v omrežje, in se odraža kot večja izpostavljenost lažnim klikom.

Če oglaševalci opazijo relativno veliko število kllikov iz takih omrežij, lahko preverijo pri svoji oglaševalski mreži, ali so že zasledili podobne primere zlorabe z istih pridruženih spletnih strani. Če se zlorabe dogajajo na določenem spletnem mestu, je verjetno oškodovanih več oglaševalcev. Oglaševalske mreže se glede zlonamernih pridruženih članov medsebojno

obveščajo in zapirajo njihove račune, ne glede na to, ali so jih pri posameznih oglaševalskih mrežah že odkrili ali ne.

Veliko število klikov, ki prihaja izven običajnega tržnega območja - Oglaševalci morajo imeti vsaj približno določeno geografsko tržno območje, na katerem delujejo njihova podjetja, in na podlagi tega spremljati IP-naslove klikov na svoje oglase. Povečano število klikov iz eksotičnih držav je za oglaševalca lahko že dober znak, da se obrne na svojega ponudnika oglaševalskih storitev in te klike reklamira. Z uporabo brezplačnih spletnih orodij, kot je www.dnsstuff.com, lahko oglaševalec preveri, iz katere države izvira določen IP-naslov. Postopek preverjanja države lahko tudi avtomatiziramo, vendar je storitev v tem primeru plačljiva. Pomanjkljivost te storitve je, da je pri IP-naslovih, ki so prijavljeni v splet preko privatnih namestniških strežnikov, odkrivanje izvorne države včasih neizvedljivo.

Nenamerni lažni kliki – Lahko se pojavijo tudi lažnii kliki na oglase, ki pa niso bili ustvarjeni z namenom, da bi se kdo z njimi okoristil ali komu škodil. Take klike imenujemo neveljavni in jih oglaševalske mreže samodejno izločajo. Vendar se lahko v oglaševalski mreži zmotijo in oglaševalcu zaračunajo kakšen neveljavni klik.

V preteklosti se je veliko oglaševalcev pritoževalo, saj so jim bili na mesečnih izpiskih računani dvojni kliki uporabnikov. Veliko starejših uporabnikov spleta je navajenih iz okolja operacijskega sistema, da je potrebno za zagon določene aplikacije dvakrat klikniti. Take klike danes vse oglaševalske mreže izločajo, vendar so še nekatere nejasnosti. Sporen je predvsem čas med obema klikoma, ki določa, ali je bil klik dvojni ali pa si je uporabnik preprosto namenoma dvakrat ogledal oglas.

Določeno število nenamernih lažnih klikov lahko sprožijo programsko vodeni spletni pajki, ki preverjajo povezave spletnih strani. Spletni pajki, ki se na strani predstavljajo z ustrezno oznako, so sicer ustrezno ignorirani in ne povzročajo težav. V vsakem primeru je smiselno upoštevati tudi to možnost, ko oglaševalec pregleduje promet na svojem spletnem mestu.

Preverjanje spletnih mest v oglaševalski mreži - Če podjetje oglašuje preko oglaševalske mreže, katere lastnik upravlja tudi s spletnim iskalnikom (npr. Google), lahko oglaševalec, če je to možno, izključi funkcijo nizanja oglasov na spletna mesta v mreži in se omeji le na tiste, ki se prikazujejo ob iskalnih zadetkih v okviru spletnega iskalnika. Tako oglaševalec lahko preveri avtentičnost klikov iz omrežja spletnih mest, vključenih v oglaševalski program. Če se pojavi velik upad sumljivih klikov, lahko oglaševalec čez nekaj časa ponovno vključi nizanje oglasov tudi na spletna mesta v omrežju in preveri, ali se sumljivi kliki znova pojavijo. Zadeva se vključi v ustrezno dokumentacijo, ki bo oglaševalcu izboljšala možnosti za povrnitev stroškov in hkrati povečala zaupanje pri oglaševalski mreži.

Prikazovanje opozorilnih sporočil - Razmeroma enostavna metoda, ki lahko učinkovito zmanjša število lažnih klikov na spletnem mestu oglaševalca, je prikaz opozorilnih sporočil. Izdelovalci programske opreme za odkrivanje lažnih klikov vključujejo v svoje aplikacije možnost prikazovanja opozoril, ki služijo preprečevanju klikanja na oglase s strani konkurentov oglaševalca. Taka sporočila so učinkovita. Ko uporabnik zagleda sporočilo, na

katerem se izpiše njegov IP-naslov z ostalimi podatki, povezanimi z njegovim računalnikom se zave, da ga nekdo spremlja, in posledično preneha z namernim klikanjem na oglase. Prikaz sporočil lahko oglaševalec nastavi z ustreznimi parametri, ki določajo, v katerih primerih se bo opozorilno sporočilo prikazalo. Primer nastavitve: oglaševalec prikaže sporočilo vsem uporabnikom, ki kliknejo na njihov oglas več kot petkrat v roku ene ure. Vanj napiše, da spremlja aktivnosti konkretnega uporabnika in da je opazil povečano število klikov na svoj oglas. Pozovemo ga, naj dejavnost prekine. Pametno je tudi, da uporabnika usmeri h kontaktni osebi v primeru, da je rensično iskal informacije o oglaševanem izdelku ali storitvi, in mu poda povezavo na spletno stran, ki jo lahko doda kot zaznamek v brskalniku.

Oglaševalci morajo poskrbeti za lastno varnost in sami pregledovati promet na svojih spletnih mestih, če želijo dodatno zavarovati svoja sredstva, namenjena za oglaševanje, in preprečiti, da bi jih oglaševalske mreže bremenile tudi za lažne klike na oglase.

Za majhna podjetja, ki imajo očitne dokaze, da na oglase klika njihov konkurent, je pametno, da se povežejo še s kakšnim drugim oglaševalcem iz iste panoge in preverijo, ali se pri njih pojavljajo isti vzorci lažnih klikov.

Zelo pomembno je, da oglaševalec shrani točna in popolna poročila ali statistične analize lažnih klikov, ki mu kasneje omogočajo ugotavljanje frekvence lažnih klikov na bolj dolgoročnem nivoju.

SKLEP

Spletno oglaševanje ima vsako leto več udeležencev, ki s svojimi investicijami na tem področju povečujejo njegovo pomembnost. Veliki zneski so pritegnili tudi zanimanje zlonamernežev in goljufov, ki se okoriščajo z zlorabo njegovih tehnoloških pomanjkljivosti, zlasti kadar temelji na plačilnem modelu CNK.

Oglaševalske mreže lažne klike težko določajo in posledično tudi izločajo, saj ni jasnih standardov, ki bi natančno opredelili lažne klike in jih jasno ločevali od veljavnih. Krovne organizacije, ki skrbijo za standarde v spletnem oglaševanju, na tem področju še niso ponudile konkretnih rešitev, ki bi zadovoljile zahteve trga.

Odkrivanje mora biti vzpostavljeno tako na strani oglaševalske mreže kot tudi oglaševalcev. Dejavnost odkrivanja lažnih klikov mora biti konstantna in vsaj korak pred izkoriščevalci spletnega oglaševanja, temelječega na plačilnem modelu CNK.

Oglaševalci se lahko poslužujejo aplikacij zunanjih neodvisnih izvajalcev, če imajo finančne zmožnosti. Funkcije za odkrivanje lažnih klikov lahko dobimo tudi vključene kot del aplikacij za opravljanje analize spletnega oglaševanja. Izobraževanje in ozaveščanje zaposlenih o problematiki lažnih klikov je enako pomembno kot njihovo odkrivanje. Oglaševalci se morajo zavedati, da lahko lažni kliki oslabijo vsako spletno oglaševalsko akcijo, zato je priporočljivo, da tudi sami z obstoječimi zmogljivostmi v podjetju odkrivajo lažne klike. Preproste metode omogočajo pregled podatkov s strežniških zapisov, kjer lahko oglaševalci pregledujejo

pogostost klikov iz posameznih IP-naslovov in geografskih področij, preko parameterizacije oglaševalskih programov lahko ugotavljajo, ali so mreže spletnih strani, kjer se nizajo oglasi, vpletene v ustvarjanje lažnih klikov, ter odkrivajo morebitne nenamerne lažne klike, ki lahko zbežijo filtrom oglaševalskih mrež.

Med načini, ki jih lahko uporabljajo oglaševalci, bom izpostavil nekaj najučinkovitejših. Povečano število klikov z istega IP-naslova lahko upravičeno vzbudi pozornost oglaševalca, saj obstaja velika verjetnost, da stoji za tem naslovom nekdo, ki želi namerno oslabiti njegovo investicijo v oglaševanje. Naslednji način, ki nam lahko pomaga pri ugotavljanju lažnih klikov, temelji na številu uporabnikov, ki hitro zapustijo oglaševalčevo spletno mesto. Zlonamerneži najraje ročno ali s pomočjo enostavnih klikbotov klikajo na oglase in takoj za tem zapirajo prikazane vsebine. Na spletnem mestu oglaševalca se to odraža kot povečano stevilo obiskovalcev, ki pa največkrat nemudoma zapustijo spletno mesto. Takšen promet mora vzbuditi sum vsakega oglaševalca. Relativno enostaven in uporaben način odkrivanja je določanje geografskega izvora klikov. Vsak oglaševalec mora imeti vsaj približno opredeljeno tržno območje, na katerem deluje, in na podlagi tega pregleduje naslove obiskovalcev, preusmerjenih s svojih oglasov. Če je med temi povečano število klikov iz držav oziroma regij izven opredeljenega tržnega območja, je potrebno take klike podrobneje analizirati in jih po potrebi tudi reklamirati pri oglaševalski mreži. Najpreprostejši in zato tudi delno učinkovit način je s prikazovanjem sporočil opozoriti uporabnika, ki namerno zaporedno klika na oglas, da nadziramo njegovo dejavnost. Slabost takih obvestil je, da gre le za opozorila, ki jih lahko uporabnik ne upošteva in so neučinkovita pri klikbotih. Ta način je edini izmed obravnavanih, ki omogoča oglaševalcu z enostavno rešitvijo aktivno preprečevati lažne klike.

Glede na pregledano dokumentacijo in literaturo ugotavljam, da trg spletnega oglaševanja ponuja še veliko prostora za programske rešitve, ki bi ustrezno ugotavljale in izločale lažne klike. Oglaševalske mreže pričakujejo predvsem več podpore iz krovnih organizacij, kjer bi morali vpeljati standarde, po katerih bi se določali lažni kliki. Trenutno si oglaševalske mreže pomagajo z lastnimi pravili in algoritmi, kar povzroča občasno spregledovanje lažnih klikov, ki na koncu bremenijo oglaševalce. Oglaševalci si ne želijo dodatnih investicij in stroškov za to, da bi preverjali že plačano storitev, vendar je to vsaj zaenkrat edina možnost, da svoje investicije ustrezno zavarujejo.

LITERATURA IN VIRI

1. *24ur.com.* Najdeno 16. januarja 2009 na spletnem naslovu http://24ur.com/.
2. *Advertise on the [Real Estate Blog]*. Najdeno 25. novembra 2008 na spletnem naslovu http://www.realestateweblog.org/real-estate-blog-ads.
3. Anupam, V., Mayer, A., Nissim, K., Pinkas, B. & Reiter, M. (1999). On the security of Pay Per Click and other web advertising schemes. *Computer Networks,* 31 str. 1091-1100.
4. *Anycount.* Najdeno 16. januarja 2009 na spletnem naslovu http://www.anycount.com.
5. Belch, G. E. & Belch, M. A. (1999). *Advertising and promotion: an integrated marketing communications perspective.* Boston: Irwin/McGraw-Hill.
6. *Cenik [Httpool]*. Najdeno 6. januarja 2010 na naslovu http://www.httpool.si/advertisers-pricelist.
7. *Cenik Oglasov [Delo]*. Najdeno 8. avgusta 2008 na spletnem naslovu http://oglasi.delo.si/download/cenik2005.pdf.
8. Cerar, L. (2004). *Uporaba interneta v trženju* [diplomsko delo]. Ljubljana : Ekonomska fakulteta.
9. *Click Fraud Detective FAQ [Click Fraud Detective]*. Najdeno 10. februarja 2009 na spletnem naslovu http://www.clickfrauddetective.com/click_fraud_detective_faq.html#faq7.
10. *Click fraud FAQ [Yahoo!]*. Najdeno 12. januarja 2009 na spletnem naslovu http://searchmarketing.yahoo.com/legal/clickfraud.php#1.
11. *Clicking Agent - A curse or myth for advertisers? [Cvanci]*. Najdeno 22. decembra 2008 na spletnem naslovu http://www.cvanci.com/articles/clicking-agent-explained.html.
12. *Digital Video In-Stream Ad Format Guidelines and Best Practices.* IAB Interactive Advertising Bureau. Najdeno 7. avgusta 2008 na spletnem naslovu http://www.iab.net/media/file/IAB-Video-Ad-Format-Standards.pdf.
13. *Formati [Iprom]*. Najdeno 14. septembra 2008 na spletnem naslovu http://www.mediaiprom.com/ index.shtml?formati.
14. Gandhi, M., Jakobsson, M. & Ratkiewicz, J. (2006). *Badvertisments: Stealthy Click-Fraud with Unwitting Accessories*. Bloomington: Indiana University.
15. *Glossary [MarketingTerms]*. Najdeno 22. septembra 2008 na spletnem naslovu http://www.marketingterms.com/dictionary/cost_per_action/.

16. *Glossary [SensaCom]*. Najdeno 15. septembra 2008 na spletnem naslovu http://sensacom.com/ web_glossary.html.

17. *Google's Adwords - Advertising Practices [Lawyers and Settlements]*. Najdeno 2. februarja 2010 na spletnem naslovu http://www.lawyersandsettlements.com/case/google_adwords.html.

18. *Google lawsuit Auction Expert International [WebOptimiser]*. Najdeno 6. februarja 2009 na spletnem naslovu http://www.weboptimiser.com/search_engine_ marketing_news/6097699.html.

19. *How will Google credit my account for invalid clicks? [Google AdWords]*. Najdeno 28. decembra 2009 na spletnem naslovu http://adwords.google.com/support/aw/bin/ answer.py?hl=en&answer=142708.

20. Hwang, J. & McMillan, S. (2005). How consumers think about interactive aspects of web advertising. *Web systems design and online consumer behavior* (str. 69-80). Najdeno 12. marca 2009 na spletnem naslovu http://www.google.com/books?hl=sl&lr=&id=J79sIVeP8M8C&oi=fnd&pg=PA69&dq=intrusive+web+ads+&ots=GVfoSNElUW&sig=gWJFJ2bWYObsq_7XUmSfHKENeuo#v=onepage&q=intrusive%20web%20ads&f=false.

21. *Industry Click Fraud Rate Hovers at 16 Percent for Third Quarter [Click Forensics]*. Najdeno 11. decembra 2008 na spletnem naslovu http://www.clickforensics.com/newsroom/press-releases/114-industry-click-fraud-rate-hovers-at-16-percent-for-third-quarter-2008-.html.

22. *Internet Advertising Revenue Report 2007 (2008)*. IAB Interactive Advertising Bureau. Najdeno 10. septembra 2008 na spletnem naslovu http://www.iab.net/ media/file/IAB_PwC_2007_full_year.pdf.

23. *Iskalnik [Google]*. Najdeno 16. januarja 2009 na spletnem naslovu http://www.google.com/.

24. Jenko, A. (2004). *Vzpon spletnega oglaševanja v Sloveniji in njegova vloga v medijskem spletu* [diplomsko delo]. Ljubljana: Ekonomska fakulteta.

25. Kaiser, S. (2007, 8. Oktober). Banner Ads: The Best Performing Banner Ad Sizes, Formats, Locations, and Colors, *WebsiteTips*. Najdeno 14. novembra 2009 na spletnem naslovu http://websitetips.com/articles/marketing/banneradsizes/.

26. Kitts, B., LeBlanc, B., Meech, R. & Laxminarayan, P. Click Fraud. Najdeno 25. aprila 2008 na spletnem naslovu http://www.asis.org/Bulletin/Dec-05/clickfraud.html.

27. Livingstone, B. (2004, 21. September). New Attacks and Defenses In Click-Fraud War. *IT Management*. Najdeno 23. oktobra 2008 na spletnem naslovu http://itmanagement.earthweb.com/ columns/executive_tech/article.php/3410931.

28. *Manuel's Web.* Najdeno 25. novembra 2008 na spletnem naslovu http://www.manuelsweb.com/images/netflix/netflix_popup2.png.

29. Mendoza, B. & Alexandrov, A. A Mechanism Design Approach to the Click Fraud Problem. *Computer Science and Engineering.* Najdeno 20. aprila 2008 na spletnem naslovu http://scholar.google.com/scholar?cluster=16579026378874013389&hl=en&as_sdt=2000.

30. Metwally, A., Agrawal, D., El Abbadi, A. & Zhengh, Q. (2006). Detecting Hit Inflation Fraud in Streams of Web Advertising Networks. *Zbornik XVI. International World Wide Web Conference* (str. 241-250). Banff: International World Wide Web Conference Committee

31. Mitchell, S. & Linden J. (2006). Click Fraud: What is it and how we make it go away?. *Think Partnership*. Najdeno 3. aprila 2009 na spletnem naslovu http://www.yoursoftcopy.com/ docs/ClickFraud.pdf.

32. Moncur, M. Web advertising basic: Understanding ad formats. Najdeno 12. aprila 2008 na spletnem naslovu http://www.wsworkshop.com/money/ad-formats.html.

33. Mordkovich, B. & Mordkovich, E. (2007). Pay-*per-click search engine marketing handbook*. ZDA: Mordcomm.

34. *MOSS - pomlad 2008.* Slovenska oglaševalska zbornica. Najdeno 22. septembra 2008 na spletnem naslovu http://www.soz.si/uploads/MOSS_Pomlad_2008_Pojasnila_k_podatkom.pdf.

35. Pagendarm, M. & Schaumburg, H. (2001). Why Are Users Banner-Blind? The Impact of Navigation Style on the Perception of Web Banners. *Journal of Digital Information*. 2 (1). Najdeno 28. septembra 2009 na spletnem naslovu http://journals.tdl.org/jodi/article/viewArticle/36/38.

36. *Pogoji in pravila [ToBoAds]*. Najdeno 13. februarja 2009 na spletnem naslovu http://www.toboads.si/sl/terms-of-service.

37. *Pop-Up Guidelines.* IAB Interactive Advertising Bureau. Najdeno 12. marca 2009 na spletnem naslovu http://www.iab.net/iab_products_and_industry_services/508676/508767/1461.

38. *Sample Reports [WhosClickingWho?]*. Najdeno 10. februarja 2009 na spletnem naslovu http://www.whosclickingwho.com/report.html.

39. Skrt, R. (2009, September). Zakaj se v Sloveniji ne splača oglaševati z bannerji?. *Moj Mikro*. Najdeno 4. decembra 2009 na spletnem naslovu http://www.nasvet.com/oglasevanje/?cp=2.

40. Soubusta, S. (2008). On click fraud. *Information wissenschaft & praxis,* 59 (2), 136-141.

41. *Spletna pasica [Datamation]*. Najdeno 25. novembra 2008 na spletnem naslovu http://itmanagement.earthweb.com/.

42. *Standards, Guidelines & Best Practices.* IAB Interactive Advertising Bureau. Najdeno 3. avgusta 2008 na spletnem naslovu http://www.iab.net/iab_products_and_ industry_services/ 508676.

43. Stricchiola, J. (2004, 29. Julij). Lost Per Click: Search Advertising & Click Fraud. *Search Engine Watch.* Najdeno 13. decembra 2008 na spletnem naslovu http://searchenginewatch.com/3387581.

44. *Terms [Wilsol]*. Najdeno 22. septembra 2008 na spletnem naslovu http://www.wilsol.net/z_terms.asp.

45. Tuzhilin, A. The Lane's Gifts v. Google Report. Najdeno 17. aprila 2008 na spletnem naslovu http://googleblog.blogspot.com/pdf/Tuzhilin_Report.pdf.

46. *Veljavni prikazi oglasov na spletni strani [ToBoAds]*. Najdeno 12. januarja 2009 na spletnem naslovu http://www.toboads.si/sl/news/potrjevanje-prikazov.

47. *VideoEgg Tries 'Cost per Engagement' [AdWeek]*. Najdeno 11. decembra 2008 na spletnem naslovu http://www.adweek.com/aw/content_display/news/digital/ e3ica0ebb59d5d28 e8c6ac4ee6233d13f31.

48. Vidyasagar, N (2004, 3. Maj). India's secret army of online ad 'clickers'. *Times of India*. Najdeno 22. decembra 2008 na spletnem naslovu http://timesofindia.indiatimes.com/ articleshow/msid-654822,curpg-1.cms.

49. Ward, S. Internet marketing. Najdeno 22. septembra 2008 na spletnem naslovu http://sbinfocanada.about.com/od/marketing/g/internetmarket.htm.

50. *Webmaster Pro.* Najdeno 25. novembra 2008 na spletnem naslovu http://www.webmasterpro.de/management/article/werbeformen-layer-ad.html/image/ Layer_ad .jpg.