Revija za kriminalistiko in kriminologijo / Ljubljana 64 / 2013 / 2, s. 195-203

Kriminalistično preiskovanje spletnih goljufij s predplačili

Igor Lamberger[1], Boštjan Slak[2], Bojan Dobovšek[3]

Spletne goljufije s predplačili, ki so v Sloveniji bolj znane kot nigerijske prevare, so v svetu umeščene med najbolj dobičkonosne goljufije. Zaradi njihove pogoste pojavnosti in prepoznavnosti jim je bilo namenjene veliko raziskovalne pozornosti, ki je botrovala nastanku obsežne literature o tej temi. Kljub temu pa je precej skop del literature, ki opisuje (ali raziskuje) odzive represivnih institucij. Naše delo skuša zapolniti to vrzel. Osrednja (kvalitativna) uporabljena metoda je pregled predvsem tuje literature. Sekundarno uporabljena kvalitativna metoda je analiza pilotske raziskave, v kateri smo intervjuvali štiri slovenske kriminaliste o obravnavani tematiki in subjektivnem zaznavanju pojavnosti tovrstnih dejanj. Literatura in vprašani kriminalisti prepoznavajo kot največji problem uporabo lažnih oziroma ponarejenih identitet v vseh obdobjih poteka prevare. Kibernetske karakteristike tovrstnih goljufij problem še povečujejo. V nasprotju s svetovno literaturo pa izprašani kriminalisti zaznavajo manjšo pojavnost dejanj, kot se ocenjuje v svetu. Pri tem opozarjamo, da gre za subjektivne zaznave.

Ključne besede: preiskovanje, nigerijska pisma, goljufije s predplačili, SPAM, kibernetska kriminaliteta

UDK: 343.37

1 Uvod

Kot vsi opisi stanja oziroma škode, ki jo naredijo goljufije, se tudi ta prispevek sooča s težavo pridobivanja natančnih podatkov o škodi in pojavnosti. Goljufije so zelo obsežen in po frekvenčnosti zelo pogost pojav, zato prav obsežnost kategorije *goljufije* (oziroma prevare) onemogoča natančen opis stanja za posamezne podtipe. To traja vse dotlej, dokler si neki specifičen podtip ne prisluži »privilegija« lastne kategorizacije, kar se največkrat zgodi z njegovo pravno kvalifikacijo oziroma zavedanjem, da ta tip kriminalitete povzroča precejšnjo škodo. Ilustrativen primer so zlorabe plačilnih kartic, ki so bile še do nedavnega zgolj del premoženjske in gospodarske kriminalitete. V kategorijo goljufije uvrščamo množico različnih dejanj, s katerimi skušajo posamezniki pridobiti protipravne premoženjske koristi. En izmed tipov so tudi t. i. *nigerijske prevare*, v tujini znane predvsem pod označbami *Nigerian scams* oziroma *419*'s, zadnje čase pa kot *Advance fee fraud*. Prav ta termin Dvoršek (2003: 383) prevaja kot *goljufije s predplačili*.

Goljufije s predplačili imajo vrsto pojavnih oblik, v osnovi pa gre za tip dejanja, v katerem oškodovanec prostovoljno izroči, nakaže ali kako drugače poravna določen znesek, za katerega verjame, da gre za vnaprejšnje plačilo za blago, storitve in/ali drugo obliko (finančne) koristi, ki pa se nikoli ne materializira (Action Fraud, 2012). Proces viktimizacije poteka tako, da oseba/osebe (storilci) ali:

— množično pošljejo elektronsko sporočilo,
— pošljejo elektronsko sporočilo na specifične naslove,
— pošljejo sporočilo specifičnemu prejemniku,
— objavijo oglas.

Besedilo elektronskega sporočila (ali oglasa) je konstruirano v takem smislu, da pri nekem številu prejemnikov aktivira uporabo določenih hevristik oziroma miselnih setov, zaradi katerih te osebe dojemajo prejeto sporočilo kot pristno (Blommaert in Omoniyi, 2006; Chang, 2008; Chang in Chong, 2010; Chiluwa, 2009; Cukier, Nesselroth, in Cody, 2007; Delio, 2002; Freiermuth, 2011; Tanfa, 2006).[4] Zaradi želje po lahkem zaslužku oziroma koristi, ki izhaja iz ponudbe v sporočilu, oseba odgovori na prejeto sporočilo in tako aktivira drugi stadij procesa, to je utrjevanje prvotne zgodbe in vpeljavo »stroškov«. Gre za »stroške« postopka, razne pristojbine, včasih celo denar za podkupnine, registracije itd. Če oseba še vedno ne posumi, da gre za prevaro preko nepreverljivih

1 Igor Lamberger, doktor ekonomskih znanosti, zaposlen na Generalni policijski upravi v Policijski akademiji kot predavatelj in zunanji sodelavec (višji predavatelj) Fakultete za varnostne vede Univerze v Mariboru. E-pošta: igor.lamberger@policija.si.

2 Boštjan Slak, mag. varstvoslovja. E-pošta: bostjan.slak@gmail.com.

3 Bojan Dobovšek, izredni profesor in prodekan na Fakulteti za varnostne vede Univerze v Mariboru. E-pošta: bojan.dobovsek@fvv.uni-mb.si.

4 Pri (večini) drugih pa se aktivira hevristično »prelepo, da bi bilo res« opozorilo (Chang, 2008).

finančnih transfernih agencij (pogosto Western Union), nakaže denar za omenjene »stroške«. Na tem stadiju se prevara konča (redko) ali pa nadaljuje (pogosteje) s tem, da prvotni pošiljatelj sporočila obvesti oškodovanca, da so nastali novi zapleti in da potrebuje še nekaj denarja za nove »stroške«. Znani so primeri, ko so osebe nakazale po več tisoč dolarjev in celo same začele izvajati kazniva dejanja, da bi lahko poplačale zahtevane »stroške« (Beaman, 2004; Delio, 2002; Mayko, 2010b). Prevara traja toliko časa, kolikor so osebe pripravljene plačevati za nove in nove »stroške« ali, dokler ne ugotovijo, da so ogoljufane. Tipi »stroškov« so odvisni od tipa sheme prevare, ki jo razvijajo prevaranti. Mi smo za potrebe članka razdelili sheme glede na tip naslovnikov.[5] Tako lahko opazimo **množično pošiljanje elektronskih sporočil,** pri čemer so tarče pravzaprav vsi, ki imajo naslov elektronske pošte. Ponudbe, ki jih dobijo, niso prilagojene interesu prejemnika sporočil. Pogosto gre tudi za vprašljive ponudbe (npr. potrebujejo žrtvin bančni račun, da nanj nakažejo denar odstavljenih diktatorjev, preplačanih javnih naročil – torej za pranje denarja). Sporočila so prilagojena trenutnim znanim razmeram (naftno bogastvo držav in s tem povezana korupcija letalske nesreče, vojna območja, nagradne igre, brezposelnost danes). Denar, ki naj bi ga dobile žrtve, pogosto izhaja iz smrti lastnikov in nihče ne zahteva dediščine za sredstva (vključno z izginulim bogastvom diktatorjev, voditeljev, vojni plen itd.); pogoste so ponudbe za dediščine »izgubljenih« in daljnih sorodnikov; ponudbe za preplačane pogodbe/kompenzacije; zadnje čase pa so pogosta obvestila o izžrebanosti na nagradnih igrah/loterijah (na katerih izžrebani sploh ne sodelujejo), obvestilo o prispelih paketih, ki jih niso nikoli naročili, oziroma jih čakajo na pošti, DHL-u, UPS-u, da poravnajo stroške (in v današnji dobi internetnega naročanja se lahko zgodi, da nekdo naroči in plača neki izdelek, ko pa dobi to lažno obvestilo o paketu, še enkrat plača lažne stroške, misleč, da gre za paket, ki ga pričakuje). Namen pošiljateljev teh sporočil je, da prepričajo oškodovanca, da bo dobil dostop do bogastva, če bo plačal stroške, provizije, pristojbine, neuradna plačila, namenil nekaj denarja za podkupnine ipd.

Malo bolj prepričljiva pri tem so **sporočila, poslana na določene naslove.** To so po navadi besedila sporočil, ki so prilagojena prejemnikovim interesom. Akademiki dobivajo na svoj naslov povabila na konference, poslovneži ponudbe za delo, študentje ponudbe za štipendije in šolnine itd. Stroški, ki jih mora oseba poravnati, vključujejo kotizacije, prijavnine, razne stroške obdelave prijave, servisa itd. **Pošiljanje sporočil določenemu prejemniku** predstavlja kombinacijo prej omenjenih tipov pošiljanja. Včasih je vsebina le minimalno prilagojena prejemniku. Najpogosteje se spremeni samo nagovor iz splošnega na osebnega (iz »dear friend« v »spoštovani gospod X Y«), in če gre za goljufivo shemo, v kateri nam daljni, a neznani »sorodnik/soimenjak« pusti veliko bogastvo, ima ta oseba isto ime/priimek (gre torej za preprosto prepričevalno metodo). Občasno se pojavljajo sporočila, ki so naslovljena na določene prejemnike, njihova vsebina pa ustreza interesnemu področju prejemnika (taka so najbolj prepričljiva). »Stroški« so kombinacija prej omenjenih možnosti (kotizacije, pristojbine, upravni postopki itd.). Pojavljajo pa se tudi **oglasi,** ki oglašujejo/prodajajo izdelek, ki ga osebe plačajo, a ga ne dobijo.

Ultrascan Research Services (mednarodna organizacija, ki se ukvarja predvsem s preučevanjem spletnih goljufij) je v svojem zadnjem poročilu nakazal, da je bilo le v letu 2009 škode, ki je izhajala iz t. i. 419[6] goljufij s predplačili škode, za kar 9,3 bilijone ameriških dolarjev (celotna ocenjena škoda do 2009 pa 41 bilijonov dolarjev), storilci so bili zaznani v najmanj 69 državah in to je bila pravzaprav najbolj uspešna oblika prevare v globalnem merilu (Ultrascan Advance Global

[5] Čeprav noben specifičen vir ne poroča o tovrstni razdelitvi prevar (po drugi strani pa se tudi ne ukvarja preveč s samim preiskovanjem) mi uporabljamo takšno porazdelitev zaradi preglednejšega opisovanja preiskovalnih metod v naslednjem delu članka. Viri, na podlagi katerih smo pridobili vpogled na sheme prevare, pa so (poleg ponudb, ki smo jih prejeli avtorji) še: Buchanan in Grant (2001); Nigerian advance fee fraud (1997); Nigerian scams (2012); Smith, Holmes in Kaufman (1999); Scamorama (www.scamorama.com); Science and technology meetings – Fraud meeting announcements (2012); Tanfa (2006); Ultrascan Advance Global Investigations (2010); Union of International Associations (2012).

[6] V 1970' letih so razvitejši del zahodnega svet poplavila pisma, v katerih so se prevaranti izdajali, da so direktorji ali računovodje, odvetniki, zdravniki (predvsem nigerijskih in zahodnoafriških) družin oziroma podjetij, ki imajo dostop do precejšnega bogastva, slednjega pa morajo spraviti iz države (zaradi državnih udarov, korupcije ipd.), pri tem pa potrebujejo pomoč naslovnika (kljub temu, da ga še nikoli niso srečali). Ogromno ljudi je nasedlo na prevaro (kljub temu, da so bila to sprva le klasična pisma naslovljena na pravne osebe, ker so bili v Afriki dostopnejši le poslovni imeniki) in škoda je bila tako velika, da so zahodne države pritisnile na Nigerijo (od koder je prišlo velika večina pisem) da kriminalizira in penalizira tovrstne prevare. Nigerija je to naredila v 419. odseku svojega kazenskega zakonika in od tod tudi eno izmed imen tovrstnih prevar (Adogame, 2009; Chang, 2008; Onyebadi in Park, 2012; Ultrascan Advance Global Investigations, 2010). Zgodbe in sheme, ki so jih takrat uporabljali, ne odstopajo preveč od dandanašnjih, ki so le modernizirane verzije. Določene nove oblike so recimo spletno nakupovanje in plačevanje storitev, ki se ne materializira, zato je potrebno biti previden pri interpretaciji statistike, ki te popolnoma nove oblike šteje k tovrstnim prevaram ali ne. Ultrascan pravi, da še ni analizirala dovolj podatkov, da bi lahko uvrstila vse tovrstne nove oblike med klasične 419 oblike prevar, se pa po do sedanjih analizah kaže velik odstotek v podporo tem mnenju (Ultrascan Advance Global Investigations, 2010). Mi po drugi strani v članku zajemamo vse spletne goljufije s predplačili.

Investigations, 2010). Mayko (2010b) opisuje redko obsodbo goljufa tovrstnih shem v primeru, kjer so preiskovalci uspeli najti 52 oseb, ki jih je ta (skupaj s sostorilci) ogoljufal v skupni škodi 1,3 milijona dolarjev.

2 Preiskovanje spletnih goljufij s predplačili

Že preiskovanje klasičnih goljufij spremlja vrsta težav in ovir, s katerimi se soočajo preiskovalci. Najpogosteje pride do ovir pri prijavi dejanja ali opustitvi prijave, saj se žrtve pogostokrat počutijo osramočene. Nekatere verjamejo, da si bodo lažje povrnile izgubljena sredstva, če storilec ne bo v zaporu. Včasih žrtve poslujejo z denarjem sumljivega izvora, v primeru nekaterih shem goljufij s predplačili pa je tudi goljufija nakazana kot nelegalna (prej omenjene oblike pranja denarja, pridobitev sredstev brez »lastnika«) (Ampratwum, 2009; Lamberger, 2005; Ndjio, 2008; Nigerian advance fee fraud, 1997; Ross in Smith, 2011; Tanfa, 2006). Prav ta nelegalni izvor denarja, skupaj z načini, kako je besedilo sporočila napisano (kjer se ustvarja vtis nujnosti in skrivnostnosti, da nekdo drug ne bi izvedel za »ponudbo«), in posledično nadaljnja korespondenca med žrtvijo in storilcem še bolj odvrne oškodovance k prijavi dejanja uradnim organom (Glickman, 2005; Schaffer, 2012; Smith, 2001; Smith et al., 1999). Drugoten velik problem preiskovanja spletnih goljufij s predplačili je kibernetska karakteristika tovrstnih prevar. Storilci oziroma pošiljatelji sporočil so zaznani po vsem svetu in danes po internetu pošiljajo sporočila na tisoče, če ne kar na milijone elektronskih predalov. Preiskovalci imajo znanje in vrsto orodij, s katerimi bi lahko storilca v določenih primerih odkrili, toda menimo, da zaradi geografske oddaljenosti med storilcem in žrtvijo nastanejo »nesorazmerni« stroški in kompleksni postopki (zaprosila INTERPOL-u in EURPOL-u, potovanja v tujino, policijska provokacija na »tujem območju« ipd.).

2.1 Pilotski vpogled v prakso preiskovanja

Za čim bolj kredibilno razpravo o preiskovanju tovrstne kriminalitete smo opravili pilotsko raziskavo, v kateri smo strukturirano intervjuvali štiri slovenske kriminaliste. Pilotski vpogled v tematiko je kritični del raziskovanja, saj omogoča testiranje uporabljenega instrumenta in metode, kjer se presoja, ali ta omogoča udeležencem dovolj možnosti izražanja, ustreznost pridobljenih podatkov in morebitne ovire (Arthur in Nazroo, 2003). Pilotski vpogled naj bi pokazal morebitne pomanjkljivosti uporabljene metode in ali smo v okvir svoje diskusije vključili ustrezno tematiko. Spoznanja bodo uporabna pri izpeljavi morebitne raziskave na ustreznejšem vzorcu. Tabela 1 predstavlja nekatere karakteristike pilotskega vzorca. Ker so prejšnje pilotske raziskave razkrile problem pridobivanja demografskih podatkov in drugih (v njihovih očeh) identifikacijskih podatkov, smo takšna vprašanja zmanjšali na minimum.

Intervjuje je opravil strokovnjak, z znanjem in delovnimi izkušnjami na področju kriminalističnega preiskovanja gospodarske kriminalitete. S tem smo dosegli večje zaupanje med intervjuvancem in izpraševalcem, ob enem pa je njegovo poznavanje tematike omogočalo lažjo (strokovno) razpravo. Pri tem smo se zavedali, da lahko to vpliva na določeno pristranskost, izhajajoč tudi iz »insajderskega« poznavanja tematike (Darlington in Scott, 2002).

V nadaljevanju članka predstavljamo primer, ki je porazdeljen na posamezne stadije razvoja prevarantske sheme. Opisujemo možne ukrepe preiskovalcev, dejavnike, ki bi jih morali upoštevati, in težave, s katerimi se srečujejo preiskovalci.

Tabela 1: Karakteristike intervjuvancev

	Delovna doba [leta]	Sektor, v katerem so delovali, ko so zaznali goljufije s predplačili	Trenutno področje dela
Intervjuvanec 1	27	gospodarska kriminaliteta	gospodarska kriminaliteta
Intervjuvanec 2	12	obveščevalna dejavnost v policiji	gospodarska kriminaliteta
Intervjuvanec 3	30	gospodarska kriminaliteta	gospodarska kriminaliteta
Intervjuvanec 4	22	gospodarska kriminaliteta	gospodarska kriminaliteta

I. stadij – pošiljanje oziroma objava oglasa

Storilci pošljejo elektronsko sporočilo, ki ni neposredno naslovljeno in katerega vsebina se ne navezuje na interesno področje prejemnika. Literatura in tudi izprašani kriminalisti navajajo, da se v takih primerih zadeve zgolj evidentirajo. Poleg tega lahko v tem stadiju preiskovalci uporabljajo le najbolj osnovne preiskovalne metode. Ker pa gre »zgolj za SPAM«, tudi nekega navdušenja tožilstva in preiskovalnih sodnikov ni mogoče pričakovati. Preiskovalci lahko pridobijo le najosnovnejše indice in nekatere namige o pošiljatelju. Z analiziranjem v sporočilu vključenih telefonskih številk lahko dobijo neke namige o lokaciji oseb. V tem primeru bi morali preiskovalci zaprositi nacionalne ponudnike telekomunikacijskih storitev, da bi posredovali podatke o osebi, na katero je prijavljen telefonski priključek. Pogosto gre za mobilne predplačniške številke, zato teh podatkov ni. Preiskovalci bi lahko v nekaterih primerih izsledili, kje je bila SIM kartica predplačniškega paketa prodana in s klasičnimi preiskovalnimi tehnikami preiskali mesto prodaje (torej kamere v bližini prodajalne, sledi papilarnih linij na denarju). Tovrstne prodajalne imajo veliko dnevnega prometa, razumno pa je tudi domnevati, da preteče mnogo časa od nakupa predplačniškega paketa, njegovega vključevanja v sporočilo in do tega, da preiskovalci izsledijo mesto prodaje, zato je obstoj teh sledi izredno malo verjeten. Ob vsem tem lahko storilci uporabljajo tudi preusmeritev klicev, pri čemer lahko številka nakazuje eno lokacijo, storilci pa so locirani nekje drugje oziroma uporabljajo tehnologijo, ki omogoča telefoniranje preko spleta (Mayko, 2010c). Intervjuvanci tudi navajajo, da se zaradi ukradenih in ponarejenih identitet, uporabljenih pri nakupu IT opreme oziroma preverjanje naročniških podatkov in podobno poizvedovanje konča v slepi ulici. Vse, kar ostane, je (realno-časovna) sledenje klica s tehnologijo, s katero razpolagajo obveščevalno-varnostne službe. Ta sledenje pa zahteva velik dokazni standard in utemeljeno nujnost ukrepa.

Podobne obrise lokacije je možno pridobiti iz elektronskega naslova, s katerega je bilo sporočilo poslano ali na katerega lahko osebe odpišejo. Elektronski naslov, če ni t. i. »spoofan« (zamaskiran oziroma lažen – kar pa je pogosto pri SPAM sporočilih), prinaša neke informacije (čas, državo izvora). Preiskovalci bi lahko zaradi veljavnih dokaznih standardov naleteli na ovire, če morajo za konkretnejše podatke zaprositi ponudnika internetnih storitev države, v katere bi jih pripeljalo primarno raziskovanje elektronskega naslova. Četudi do zaprosila pride, se preiskava redko uspešno razvije, saj se za dostop do spleta uporabljajo predplačniški paketi oziroma sta IT oprema in naročnina pridobljena z ukradenimi ali ponarejenimi identitetami. Analiza besedila (forenzična, grafološka ipd.) v večini primerov ne prinaša nobenih uporabnih spoznanj.

Preiskovalci bi sicer lahko odgovorili na sporočilo in nekako igrali vlogo naslovnika, nadaljnja korespondenca pa bi lahko prinesla uporabnejša spoznanja, vendar se moramo zavedati, da pošiljanja sporočil včasih ne izvajajo tiste osebe, s katerimi si kasneje oškodovanec dopisuje (Delio, 2002). Poleg tega bi potem morali zopet zaprositi tuje organe za pomoč, in kot poudarjajo intervjuvanci, se tu pojavlja vrsta vprašanj pravne narave. Če bi preiskovalec smel in celo razvil shemo tako daleč, da bi sam nakazal denar, bi sicer lahko teoretično prijeli osumljenca, če bi upoštevali vrsto dejavnikov in dobili pomoč od agencije, ki bi bila uporabljena za izvedbo transakcije (morali bi vedeti, katero poslovalnico bo osumljenec obiskal, prav tako pa bi zaposleni na tej agenciji morali signalizirati oziroma sporočiti policiji v zasedi, kdo je prevzel denar). To bi verjetno vodilo v upad dobička, zato tovrstnim agencijam to ni v interesu.[7] Ob vsem tem se pojavlja vprašanje policijske provokacije po spletu. Intervjuvanci so še posebej izpostavili problem tovrstnih finančnih posredovalnic, saj oseba ne potrebuje za dvig denarja nobenega dokumenta, poznati mora le pravo geslo.

Tudi takrat, ko *oseba prijavi sporočilo, ki sicer ni neposredno naslovljeno nanjo, po vsebini pa je v prejemnikovem interesu,* se preiskovalci srečajo s podobnim setom problemov. V takem primeru je mogoče sklepati, da je bil seznam naslovnikov odtujen od nekaterih, javnosti sicer nedostopnih baz, ali pa iz javno dostopnega portala, ki se ukvarja z interesnim področjem prejemnikov. V vsakem primeru se preiskovalec sooči z že prej napisano situacijo omejenih preiskovalnih ukrepov (še vedno gre za problem naklepa in »resnosti«). Toda prilagojena vsebina je lahko indic, še predvsem, če je nekdo šele začel prejemati tovrstna sporočila po nekem dogodku (npr. akademik po prijavi na konferenco, nezaposleni po prijavi na agencijo za zaposlovanje, iskalec stikov po internetu, prodajalec različnih storitev/izdelkov). Če so v sporočilu omenjene osebe in življenjepisi v kombinaciji z neko organizacijo, se je včasih smotrno pozanimati pri teh osebah, ali so kdaj res sodelovale pri teh organizacijah, kdo je imel stik z njimi in podobno. Seveda je tu vprašanje smotrnosti tovrstnega povpraševanja in kaj to pomeni za nadaljnje preiskovanje.

Prav nič drugače ni, ko *oseba prijavi sporočilo, ki je bilo naslovljeno izključno nanjo.* Edina razlika je večja izraženost naklepa, saj je tu pošiljatelj izrecno določil osebo, ki jo želi ogoljufati. Nagovor v sporočilu v večini primerov ne pove ničesar, (saj lahko nekdo razbere ime prejemnika iz elektronskega naslova) razen če je naslovnik naveden z imenom ali/in priimkom, elektronski naslov pa tega ne razkriva. Tu se zopet pojavi neki indic o izvoru oziroma dostopanju do neke

[7] Ultrascan celo navaja, da so tovrstne agencije v lasti organiziranih skupin (Ultrascan Advance Global Investigations, 2010).

baze podatkov, kjer so te informacije shranjene. Problem obstaja, ker se danes ljudje skoraj dnevno registriramo na vrsto portalov in zelo težko je najti tistega, od katerega informacije odtekajo. Iskanje pa je olajšano, če je vsebina prilagojena prejemniku in je tudi nagovor personaliziran. V tem primeru je to zopet dober indic, da je bil naslov odtujen z neke specializirane podatkovne baze. Storilci lahko seveda poberejo elektronske naslove in potem ročno ali po sprogramiranih skriptah, Excel formulah ipd. množično personalizirajo nagovore sporočil s podatki, razvidnimi iz elektronskih naslovov. Če je personalizacija podrobnejša (npr. ravno pridobljen doktorski naziv), to kaže, da podatki odtekajo oziroma prevaranti dostopajo do portalov, kjer so te informacije ažurno objavljene. To pomeni, da je smotrno pregledati in spremljati promet na tovrstnih straneh. Pojavijo pa se vprašanja dokaznega standarda, ki je potreben, da lahko preiskovalci preko tožilca in preiskovalnega sodnika zaprosijo za takšne podatke.

Redkeje se zgodi, da osebe *prijavijo neki sumljiv oglas* zgolj po prebranem v oglasu (izjeme so vpleteni mladoletni, kriminaliteta spolne zlorabe, prodaja živali in nevarnih snovi), poleg tega pa moderatorji spletnih oglaševalskih portalov dokaj ažurno spremljajo objavljene oglase. V nekaterih primerih policija sama pri »patruljiranju po internetu« naleti na sumljiv oglas in potem reagira. Vsekakor pa je naklep in posledično motiv težko »dokazati« zgolj iz besedila oglasa. Uspešnost nadaljnjih ukrepov je odvisna od kakovosti spletne strani (katere podatke zahteva za prijavo in objavo) in vrste sledi, ki jih je storilec pustil v oglasu. Resnejše strani zahtevajo vpis podatkov plačilnih kartic, celo sliko osebnega dokumenta, druge zgolj elektronski naslov. To seveda privede do enakih, že prej opisanih težav. Ob vsem tem je treba upoštevati še to, da so podatki, ki so bili uporabljeni v sporočilu, lahko produkt kraje identitete (in to velja za vse prevarantske sheme). Avtorji člankov, ki obravnavajo tematiko goljufij s predplačili, opozarjajo, da potem, ko nekdo odgovori na sporočilo in res pošlje neke osebne podatke (ali celo sliko), prevaranti te podatke uporabijo za druge goljufije (Schaffer, 2012; Wells, 2004; Tanfa, 2006;).

II. stadij – oseba odgovori na sporočilo, razvije korespondenco s prevaranti, potem pa spozna, da gre za sumljivo zadevo (pred nakazilom denarja)

Glede na intenzivnost in trajanje korespondence ta stadij prinaša določena uporabna spoznanja k prej omenjenim podatkom. Pri tem se ne sme zanemariti, da je lahko oseba, s katero nekdo komunicira, v eni državi, denar pa je kasneje nakazan v tretjo državo. Prav tako lahko čas odgovorov kaže, kje je oseba, čeprav gre mnogokrat za organizirano skupino (Glickman, 2005; Mayko, 2010b; Ross in Smith, 2011; Tanfa, 2006),[8] ki dela 24 ur na dan in tako so odgovori precej pravočasni. Pridobijo se lahko indici, od kod so pridobili podatke o naslovniku (ime, naziv, elektronski naslov). Pojavijo se lahko indici od prejšnjih prevar (ime, drugi osebni podatki, slika dokumentov ipd. »našega dopisovalca«, ki pa so produkt prejšnjih prevar). V tem stadiju prevaranti pogosto pošiljajo skenirane kopije pogodb, certifikatov in podobnih uradnih dokumentov, da bi s tem dodatno prepričali korespondente. Nekatere pogodbe delujejo tako pristno zato, ker so pristne (Buchanan in Grant, 2001).[9] Možna je analiza teh pogodb, da bi preverili izvor oziroma kako so prevaranti pridobili vzorec pogodbe. Takšne kriminalistično-taktične in kriminalistično-tehnične preiskave dokumentov so pri preiskovanju goljufij lahko dober vir različnih sledi (Dvoršek, 2003). V državah, kjer je korupcija izredno razširjena, to ne privede do velikih uspehov. Največkrat opozori na nekatera varnostna vprašanja npr. nigerijskih in zahodnoafriških bank, kar pa se tako ali tako že sami zavedajo. Pri tem je izraženost naklepa še večja, a so preiskovalci kljub temu še vedno pred veliko oviro. Še vedno bi bila potrebna širša preiskava na področju več držav, angažiranje strokovnjakov kibernetske kriminalitete in večja časovna predanost primeru – da bi lahko preiskovalec nadaljeval korespondenco in pripravil ozadje za kontrolirano pošiljko, navidezen odkup/prodajo, izplačilo, odvisno od sheme prevare.

III. stadij – oseba prijavi dejanje, ko je že bila oškodovana

Intervjuvani kriminalisti so poudarili, da je največ prijav dejanj prav v tem stadiju prevare, ko se storilci oškodovancem ne oglašajo več. Tu je izraženost naklepa že popolnoma jasna, prisoten je motiv, a so sledi še vedno minimalne. Poleg že vseh prej navedenih sledi so edine nove sledi neko ime ali neki priimek, uporabljen pri korespondenci (a pogosto popolnoma lažen), ter neka identifikacijska označba osebe, kateri je bil nakazan denar. Večinoma se posluje preko agencij, kjer je za dvig denarja dovolj poznati geslo za dostop, zato je sledljivost osebe, ki je prevzela denar, skorajda nemogoča (sploh,

[8] Buchanan in Grant (2001) pišeta, da gre za organizirane skupine, katerih hierarhija je ohlapnejša, kot pri recimo klasičnih organiziranih skupinah. Sploh pa je organiziranost videna preko določenih shem, ko se recimo oškodovanec poveže s kakimi poslovneži iz bližine oziroma držav, ki izžarevajo večjo zaupljivost, ali ko oškodovanca povabijo na obisk v tujo državo (ali tudi domačo), kjer ga nastanijo v dobrih hotelih, dodelijo osebnega šoferja in uredijo obisk modernih poslovalnic (Buchanan in Grant, 2001).

[9] Ampratwum (2009) celo poroča o tem, da so se pojavile kritike nigerijske državne uprave, ker naj bi goljufom posodila pisarne in telekomunikacijsko opremo, saj naj bi bile tovrstne goljufije tretji najbolj dobičkonosen posel Nigerijcev. Podobno pišeta Buchanan in Grant (2001) glede bank in kako prevaranti zmanipulirajo ukradene čeke (ponarejajo, prilagajajo).

če temu dodamo koruptivnost zaposlenih v teh agencijah, ki so za določen odstotek pripravljeni kršiti pravila). Če bi preiskovalci pripravili zasedo, bi bilo prijetje seveda uspešnejše, vendar je to skorajda nemogoče.

Iz vsega napisanega je razvidna vrsta težav, med katerimi najbolj izstopajo lažne in namišljene identitete, ki se uporabljajo za zakup in uporabo IT opreme, korespondenco in tudi za dvig denarja. Gre za globalno prepoznan problem in tudi drugje se srečujejo z njim (glej na primer Mayko, 2010a). Vsi intervjuvani kriminalisti so večkrat omenili ta problem. Primarni je torej neprepoznavnost storilca, v katerega bi lahko usmerili nadaljnje preiskovalne postopke, ki bi botrovali k potrditvi/ovržbi suma. Dvoršek (2003) navaja, da lahko preiskave prostorov osumljencev goljufij prinesejo vrsto sledi, saj se za izpeljavo goljufij potrebuje veliko lažne, ponarejene ali ukradene dokumentacije. Pri goljufijah, ki že po svoji naravi zahtevajo obsežno korespondenco med oškodovancem in storilcem, obstaja možnost odkritja sledi tovrstne komunikacije. Dandanes zaradi kibernetskih karakteristik, tudi uporabe elektronskih naprav za izpeljavo goljufij, obstaja vrsta sledi v digitalni obliki, a le-te se prav tako najpogosteje najde prav pri hišni preiskavi (Dimc in Dobovšek, 2012). Iz primera obsojenega goljufa, ki ga opisuje Mayko (2010a), je razvidno, da je goljufa, ki si je ameriško državljanstvo pridobil s poroko, pravzaprav izdala ogromna količina elektronskih naprav, ki jih je imel pri sebi na potovanju med Nigerijo in ZDA. Šele preiskava vsebin naprav je razkrila in potrdila, za katero vrsto goljufije gre. Iz napisanega se poraja tudi vprašanje, če nemara ta uspešna preiskava ni bila produkt represivnejšega pristopa in pravnega okvira, ki velja v ZDA.

V naši raziskavi so intervjuvani kriminalisti enotno menili, da gre za obliko organizirane kriminalitete in celo za precej dobro organizirano dejavnost. Zanimivo je, da kljub vsemu – po subjektivni oceni kriminalistov – v Sloveniji ni veliko tovrstnih primerov, da pa škoda, ko pride do dejanja, sega tudi do nekaj tisoč evrov. Ko smo jih povprašali po subjektivni oceni »psihične« škode, smo dobili odgovore, da so žrtve razočarane, osramočene, pa tudi prestrašene, kar je pri nekaterih tudi razlog za prijavo. Dobili smo tudi zanimiv odgovor, da so med žrtvami tudi *hazarderji, ki so tvegali in niso pretirano razočarani* (intervjuvanec 1) – vidik, ki bi ga bilo dobro podrobneje raziskati. Med ostalimi razlogi, zakaj osebe sploh prepričajo takšne ponudbe, pa kriminalisti navajajo naivnost, altruistično naravnanost oseb, idejo o lahkem zaslužku in pohlep. Kot poglavitno metodo preventivne dejavnosti intervjuvanci navajajo osveščanje javnosti, kjer bi to nalogo največkrat zaupali medijem, policiji in šolam, sledijo pa razni uradi in inšpektorati, katerih domena dela je zaščita potrošnikov. Vloge medijev vsekakor ne gre zanemariti, saj dokazano vplivajo na strah pred kibernetsko kriminaliteto in na razumevanje kibernetske kriminalitete (Bernik in Meško, 2011).

Intervjuvanci prav tako vidijo preiskovanje kot nalogo kriminalistov in menijo, da so tudi v tujini kriminalisti tisti, ki se ukvarjajo s tovrstnim preiskovanjem, ne izpostavijo pa, ali gre za kriminaliste v klasičnem smislu ali kriminaliste posebnega oddelka za pregon kibernetske kriminalitete. Ustanovitev tega oddelka si Slovenija po mnenju Bernika in Prislanove (Bernik in Prislan, 2012) ne more privoščiti, vsaj ne v takšni obliki, kot ga imajo večje države.

Razvidno je, da gre pravzaprav za zelo preprosto prevaro, ki izkorišča pohlep, neprevidnost, osebne interese ljudi in pa kaotičnost, močno razširjenost korupcije in brezpravnost v neki državi. Kljub temu, da vsaj na prvi pogled v Sloveniji ne obstajajo empirično podprti dokazi o veliki obsežnosti tovrstnih dejanj, bi bilo vredno razmisliti o prihodnjem trendu tovrstnih goljufij, in to predvsem s stališča motivacije. Kigerl (2012) navaja, da stopnja nezaposlenosti v dani državi sicer ni pomembno povezana s SPAM dejavnostjo, po drugi strani pa ugotavlja, da je nezaposlenost pomembno povezana z *interakcijo* s SPAM dejavnostmi, za kar obstajata razloga: a) nezaposlenost motivira osebe, da storijo kazniva dejanja (torej preko pošiljanja SPAM) in b) nezaposleni preživijo več časa na spletu in so tako lahko žrtve SPAM prevar. Pri tem opozarja, da pravzaprav obstaja vrsto metodoloških ovir za neizpodbitnost ugotovitev, in sicer težave locirati izvor SPAM pošte, vprašanje, ali nezaposlenost v neki državi dejansko vpliva na (ne)zaposlenost informacijsko-tehnoloških strokovnjakov, ki so tisti, katerih znanje omogoča tovrstno pošiljanje SPAM pisem in izvajanje kibernetskega kriminala. Vprašanje je tudi, ali osebe, ki izvajajo tovrstna dejanja, dejansko ne potrebujejo uradnega izobraževanja. Razpravo zaključuje, da lahko le v nekaterih primerih nezaposlenost poveča stopnjo kibernetske kriminalitete (ibid.). Pri tem deluje nezaposlenost dvodimenzionalno, ker po eni strani oseba zaradi nezmožnosti drugačne pridobitve dohodkov začne izvajati kibernetsko obarvana kazniva dejanja za »golo« preživetje, po drugi strani pa so lahko kibernetsko obarvana kazniva dejanja tudi način izražanja nezadovoljstva z in *do* razmer v družbi (Peršak, 2009). Nezaposlenost študentov in izobraženih oseb je po mnenju nekaterih avtorjev (Dixon, 2005; Igwe, 2010; Salu, 2005) pravzaprav rodila nigerijske prevare, kjer pa poleg na tak način pridobljenega denarja oziroma iz tega izhajajoča sredstva posredno omogočajo večjo socialno privlačnost (Okonkwo, 2013). Motivacija za izvajanje goljufij in prevar pa je lahko tudi občutek premetenosti, spretnosti in večvrednosti (Kanduč, 2009; Smith, 2001; Tanfa, 2006) – nekaj, kar je mogoče zaslediti že v času grškega imperija (Tičar, Bohinc in Nahtigal, 2010). Brezposelnost kot motivacijski dejavnik pri izvajanju kibernetsko obarvanih kaznivih dejanj prepoznavata tudi Bernik in Prislan (2012). Kakšno je torej tovrstno tveganje za Slovenijo, ki ima ob visoki stopnji splošne nezaposlenosti tudi mnogo nezaposlenih visoko izobraženih oseb?

3 Zaključek

Članek odseva dokaj realistično-pesimistično stanje preiskovanja goljufij s predplačili. Razvidna je vrsta problematik, ki toliko otežujejo preiskovanje, da je število uspešno raziskanih primerov zelo majhno. Le en izprašani kriminalist je omenil, da pozna primer odkritja *skupine storilcev na Nizozemskem, ki je oškodovala našega državljana, kazenska ovadba pa je bila podana tam* (intervjuvanec 3). Večina primerov se sicer ne razvije do te faze, predvsem zaradi fiktivnih identitet. Ugotovili smo, da si trije od štirih izprašanih kriminalistov kot *goljufije s predplačili* predstavlja dejanja, ko nekdo plača nek predmet/storitev vnaprej in tega ne dobi, kar je v tujini in angleščini poznano kot *non-delivery fraud*. Termin *nigerijska pisma* kriminalisti okarakterizirajo z vsemi globalno prepoznanimi lastnostmi in značilnostmi teh dejanj. Tako pridemo v položaj, ko se moramo vprašati, koliko obsežna naj bo kategorija goljufij s predplačili in katere podtipe goljufivih shem naj vključuje. Vprašati se moramo tudi, ali naj sledimo zgledom, ki v *goljufije s predplačili* vključujejo tipe dejanj, kjer oseba plača za storitev/predmet, a plačanega ne dobi. Ali je sploh smiselno določati podtipe? Ali si niso dejanja (podtipi) navsezadnje izredno podobna, če ne kar enaka?

Prav tako lahko razpravljamo o intenzivnosti preiskovalnih ukrepov. Poznamo vrsto tehnoloških in informacijskih metod, ki bi prinesle veliko in raznoliko vrsto sledi, a se smejo uporabljati pod okriljem visokega dokaznega standarda oziroma v t. i. kibernetskem vojskovanju. Govorimo o vdoru v elektronske naprave storilcev goljufij s predplačili. Tak vdor (občasno precej lahko izvedljiv, glede na to, da goljufi zaprosijo za mnoge podatke, pri čemer se ustvarja vrsta datotek in priponk, med katere bi lahko skrili programsko kodo za vstop v sistem goljufove elektronske naprave) ni niti pravno zakonit niti legitimen. Avtorji se s tem strinjamo, saj ohranjanje posameznikove čim večje intimne sfere nadvlada potencialno korist pri preiskovanju tovrstnih kaznivih dejanj.

Med metodami, ki so na voljo, brez dvoma prevladuje mednarodno sodelovanje (Bernik in Prislan, 2012), *v katerega* ali *iz katerega* vodi digitalna forenzika (Dimc in Dobovšek, 2012). Kljub temu, da elektronske naprave in splet predstavljajo in vsebujejo vrsto dokazov elektronske narave, lahko te sledi vodijo v slepo ulico (Bernik in Prislan, 2012). Intervjuji in literatura nakazujejo, da se digitalna forenzika pri spletnih goljufijah s predplačili le redko izkaže z uporabnimi spoznanji, saj pravzaprav niti ne moremo aplicirati vseh njenih zmožnosti.

Ob vsem napisanem je iluzorno pričakovati, da se bo obsežnost literature, ki se ukvarja s preiskovanjem tovrstne kriminalitete, kaj spremenila (nekaj, kar velja za gospodarsko kriminaliteto nasploh). »Akademski kriminalisti« sicer lahko ponudimo/ponujajo vrsto idej in teorij, ki pa jih je bilo treba soočiti s praktičnim znanjem in predvsem izkušnjami kriminalistov, ki se skoraj vsak dan ukvarjajo s tovrstno in podobno vrsto kriminalitete. Pri tem se srečamo z novim problemom, to je izdajanje preiskovalnega know-how. Avtorji menimo, da bi bilo smotrnejše razvijati posebne preiskovalne postopke pri preiskovanju goljufij (in gospodarske kriminalitete) v timskem sodelovanju med preiskovalci, akademiki in družboslovnimi znanstveniki. V javnosti bi bilo treba predstavljati najbolj generična spoznanja, ki bi po eni strani zadovoljila tiste, ki jih tovrstni pojavi zanimajo, in spodbudila brainstorming, ki bi ustvarjal nove preiskovalne prijeme.

Literatura

1. Action Fraud. (2012). *Advance fee fraud*. Pridobljeno na http://www.actionfraud.police.uk/fraud-az-advance-fee-fraud
2. Adogame, A. (2009). The 419 code as business unusual: Youth and the unfolding of the advance fee fraud online discourse. *Asian Journal of Social Science 37*(4), 551–573.
3. Ampratwum, E. F. (2009). Advance fee fraud »419« and investor confidence in the economies of sub-Saharan African (SSA). *Journal of Financial Crime, 16*(1), 67–79.
4. Arthur, S. in Nazroo, J. (2003). Designing fieldwork strategies and materials. V J. Ritchie in J. Lewis (ur.), *Qualitative research practice: A guide for social science students and researchers* (str. 109–137). London, Thousand Oaks, New Delhi: Sage.
5. Beaman, L. (2004). Adviser falls for Nigerian letter scam. *Money Management*, *18*(11), 11.
6. Bernik, I. in Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, *62*(3), 242–252.
7. Bernik, I. in Prislan, K. (2012). *Kibernetska kriminaliteta, informacijsko bojevanje in kibernetski terorizem*. Ljubljana: Fakulteta za varnostne vede.
8. Blommaert, J. in Omoniyi, T. (2006). Email fraud: Language, technology, and the indexicals of globalisation. *Social Semiotics, 16*(4), 573–605.
9. Buchanan, J. in Grant, A. J. (2001). Investigating and prosecuting Nigerian fraud. *United States Attorneys' Bulletin 49*(6), 39–47.
10. Chang, J. J. (2008). An analysis of advance fee fraud on the internet. *Journal of Financial Crime, 15*(1), 71–81.
11. Chang, J. J. in Chong, M. D. (2010). Psychological influences in e-mail fraud. *Journal of Financial Crime, 17*(3), 337–350.
12. Chiluwa, I. (2009). The discourse of digital deceptions and '419' emails. *Discourse Studies, 11*(6), 635–660.
13. Cukier, W., Nesselroth, E. J. in Cody, S. (2007). Genre, narrative and the "Nigerian letter" in electronic mail. V *Proceedings of the 40th Annual Hawaii International Conference on System Sciences. Big Island, Hawaii.*
14. Darlington, Y. in Scott, D. (2002). *Qualitative research in practice: Stories from the field.* Crows Nest: Allen & Unwin.
15. Delio, M. (17. 7. 2002). Meet the Nigerian e-mail grifters. *Wired.* Pridobljeno na http://www.wired.com/culture/lifestyle/news/2002/07/53818?currentPage=all
16. Dimc, M. in Dobovšek, B. (2012). *Kriminaliteta v informacijski družbi.* Ljubljana: Fakulteta za varnostne vede.

17. Dixon, R. (20. 10. 2005). Nigerian cyber scammers. *Los Angeles Times*. Pridobljeno na http://www.latimes.com/la-fg-scammers-20oct20,0,7125847.story?page=1
18. Dvoršek, A. (2003). *Kriminalistična metodika.* Ljubljana: Ministrstvo za notranje zadeve, Visoka policijsko-varnostna šola.
19. Freiermuth, M. R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication, 5*(2), 123–145.
20. Glickman, H. (2005). The Nigerian »419« advance fee scams: Prank or peril? *Canadian Journal of African Studies, 39*(3), 460–489.
21. Igwe, C. N. (2010). Socio-economic developments and the rise of 419 advance-fee fraud in Nigeria. *European Journal of Social Sciences 20*(1), 184–193.
22. Kanduč, Z. (2009). Prevare, prevarantstvo in prevaranti: preliminarna kriminološka analiza. *Revija za kriminalistiko in kriminologijo*, *60*(3), 223–237.
23. Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470–486.
24. Lamberger, I. (2005). Mednarodne finančne goljufije. V A. Dvoršek, in L. Selinšek (ur.), *Problematika finančnega kriminala v Sloveniji* (str. 87–100). Ljubljana: Fakulteta za policijsko-varnostne vede; Maribor: Pravna fakulteta.
25. Mayko, M. P. (1. 9. 2010a). Nigerian man gets prison time for e-mail scam. *Connecticut Post.* Pridobljeno na http://www.ctpost.com/default/article/Nigerian-man-gets-prison-time-for-e-mail-scam-641246.php
26. Mayko, M. P. (3. 5. 2010b). Nigerian scams still net victims. *Connecticut Post.* Pridobljeno na http://www.ctpost.com/local/article/Nigerian-scams-still-net-victims-472312.php
27. Mayko, M. P. (9. 5. 2010c). Sentencing delayed for Nigerian scammer. *Connecticut Post.* Pridobljeno na http://www.ctpost.com/default/article/Sentencing-delayed-for-Nigerian-scammer-480161.php
28. Ndjio, B. (2008). *Cameroonian feymen and Nigerian '419' scammers: Two examples of Africa's 'reinvention' of the global capitalism*. Leiden: African Studies Centre.
29. *Nigerian advance fee fraud.* (1997). U.S. Department of State. Pridobljeno na www.state.gov/www/regions/africa/naffpub.pdf
30. *Nigerian scams*. (2012). Pridobljeno na http://www.crimes-of-persuasion.com/Crimes/Business/nigerian.htm
31. Okonkwo, A. D. (2013). Generational Perspectives of Unprotected Sex and Sustainable Behavior Change in Nigeria. *SAGE Open,* (Jan.-Mar.), 1–18.
32. Onyebadi, U. in Park, J. (2012). 'I'm Sister Maria. Please help me': A lexical study of 4-1-9 international advance fee fraud email communications. *International Communication Gazette, 74*(2), 181–199.
33. Peršak, N. (2009). Virtualnost, (ne)moralnost in škodljivost: normativna vprašanja nekaterih oblik kibernetične kriminalitete. *Revija za kriminalistiko in kriminologijo*, *60*(3), 191–198.
34. Ross, S. in Smith, R. G. (2011). Risk factors for advance fee fraud victimization. *Trends & Issues in Crime and Criminal Justice,* (420). Pridobljeno na http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi420.aspx
35. Salu, A. O. (2005). Online crimes and advance fee fraud in Nigeria - are available legal remedies adequate? *Journal of Money Laundering Control, 8*(2), 159–167.
36. Schaffer, D. (2012). The language of scam spams: Linguistic features of »Nigerian fraud« e-mails. *ETC.: A Review of General Semantics, 69*(2), 157–179.
37. *Science and technology meetings – Fraud meeting announcements*. (2012). Group on Earth Observations. Pridobljeno na http://www.geo-tasks.org/meetings_sandt/fraud_meetings.php
38. Smith, D. J. (2001). Ritual killing, 419, and fast wealth: Inequality and the popular imagination in southeastern Nigeria. *American Ethnologist, 28*(4), 803–826.
39. Smith, R. G., Holmes, M. N. in Kaufman, P. (1999). Nigerian advance fee fraud. *Trends & Issues in Crime and Criminal Justice,* (121).
40. Tanfa, D. Y. (2006). *Advanced fee fraud* (Doctoral dissertation). Univerzety of South Africa.
41. Tičar, B., Bohinc, R. in Nahtigal, M. (2010). Recepcija rimske antične vrednote fides – poštenosti in zvestobe dani besedi – v sodobnem slovenskem upravnem pravu. *Acta Histriae, 18*(4), 847–864.
42. Ultrascan Advance Global Investigations. (2010). *419 advance fee fraud statistics 2009.* Prevzeto 26. Junij 2012 iz Ultrascan Advance Global Investigations: http://www.ultrascan-agi.com/public_html/html/aff_37_countries.html
43. Union of International Associations. (2012). *Monitoring fraudulent announcements*. Pridobljeno na http://www.uia.be/fraud_monitor
44. Wells, J. T. (2004). Foreign advance-fee scams. *Journal of Accountancy.* Pridobljeno na http://www.journalofaccountancy.com/Issues/2004/Apr/ForeignAdvanceFeeScams.htm

Criminal Investigation of Advance Fee Fraud

Igor Lamberger, Ph. D. in Economic Sciences, employed at the General Police Directorate,
Lecturer at Slovenian Police academy and an external consultant (Senior Lecturer)
at Faculty of Criminal Justice and Security studies, University of Maribor, Slovenia. E-mail: igor.lamberger@policija.si.

Boštjan Slak, M.A. in Criminal Justice and Security. E-mail: bostjan.slak@gmail.com.

Bojan Dobovšek, associate professor and Vice-Dean of the Faculty of Criminal Justice and Security,
University of Maribor, Slovenia. E-mail: bojan.dobovsek@fvv.uni-mb.si.

Advance fee fraud, or in Slovenia more known as Nigerian scams, are ranked among the world's most profitable frauds. Because of their frequency and visibility, these types of fraud received academic and scientific attention, which led to an accumulation of large amounts of literature. However, the scope of the literature that describes (or researches) the responses of repressive institutions are rather vague. Our work attempts to fill this gap. The primary (qualitative) research method utilized was a review of the literature while secondary qualitative research method was the analysis of a pilot study in which four Slovenian criminal investigators were interviewed. They were asked about the issues and their subjective perception about the frequency of occurrence of these acts. Literature and interviewed investigators indicate the biggest problem is the use of false or falsified identities, which are used in all stages of the frauds. Cyber characteristics of these types of fraud amplify these problems even more. Contrary to worldwide literature, the interviewed investigators perceive a lower incidence of offenses, as estimated worldwide. However as warned, this is a subjective perception.

Keywords: investigation, Nigerian letters, advance fee frauds, SPAM, cyber crime

UDC: 343.37