Др Владимир Урошевић
Министарство унутрашњих послова Србије - УКП, СБПОК,
Мр Звонимир Ивановић
Криминалистичко – полицијска академија, Београд

УДК: 004.738.5
Примљено: 23. јануар 2010.
Стручни чланак

УЛОГА ИНТЕРНЕТА КОД АНГАЖОВАЊА ПОСРЕДНИКА У ПРЕУЗИМАЊУ ПРОТИВПРАВНО ПРИБАВЉЕНЕ РОБЕ И НОВЦА ИЗВРШЕЊЕМ КРИВИЧНИХ ДЕЛА ВИСОКОТЕХНОЛОШКОГ КРИМИНАЛА

Због начина на који функционише Интернет пружа извршиоцима кривичних дела из области високотехнолошког криминала прилагодљив и практичан амбијент за извршење кривичних дела, уз велике могућности за скривање идентитета. Најрањивији тренутак за извршиоце кривичних дела, који користе благодети интернета у злоупотреби платних картица, је тренутак у коме су принуђени да преузимају противправно стечени новац или робу. Да би избегли да буду откривени приликом трансфера новца или робе или њиховог преузимања извршиоци кривичних дела из ове области ангажују већи број лица, различитих интересовања и социјалног статуса, која доводе у заблуду да им помогну да подигну робу или новац преко својих рачуна у њихово име, уз одређену надокнаду (или из неких других, најчешће емотивних разлога), те да им тај новац или робу након тога пошаљу на унапред одређени рачун или адресу. Ова лица врло често нису свесна која је њихова улога и у заблуди су да раде легалан посао, што даје посебну димензију овом акту како за извршиоца тако и за жртву заблуде. Методом социјалног инжињеринга преко Интернета свакодневно се ангажује велики број лица за ове сврхе, а са појавом социјалних мрежа овај вид скривања идентитета извршилаца, у овој фази извршења кривичних дела, доживео је значајну експанзију. Корисници Интернета у Републици Србији такође су изложени ризику који настаје као последица наведених криминалних активности извршилаца кривичних дела из области високотехнолошког криминала.

***Кључне речи**: компјутерска превара; превара са кредитним картицама; "money mules"; друштвени инжињеринг; високотехнолошки криминал у РС.*

I. УВОД

Ангажовање лица од стране извршилаца кривичних дела за трансфер дроге, оружја, новца и сл., је веома позната активност добро организованих криминалних група, а лица која преносе предмете кривичних дела и подижу новац за одређени проценат на енглеском језику у литератури се називају „*money mule*“

што у слободном преводу значи „мазге за пренос новца“[1]. Са појавом Интернета ангажовање лица за подизање противправно стечене робе или новца насталог извршењем кривичних дела из области високотехнолошког криминала постала је глобално распрострањена појава. Приликом откривања кривичних дела и њиховог проналаска највећи број ових лица не може да пружи валидне (а понекада икакве) податке о правом извршиоцу кривичног дела који је од њих сакрио свој идентитет или дао лажни идентитет при комуникацији на Интернету.

Учествовање у преварама овог типа и у трансферу новца и робе може довести до покретања преткривичног поступка против лица које није свесно своје улоге, а може и да буде осумњичено да је члан организоване криминалне групе чија је улога била прање новца. Овакве активности нису прихватљиве ни за банкарске системе и често воде до укидања рачуна корисника, након чега се нарушава пословни углед клијента који се иначе врло тешко враћа, а такође и до негативних извештаја у кредитном бироу чиме се може знатно отежати и положај и живот човека.

При ангажовању лица за ову улогу извршиоци кривичних дела користе различите методе[2] од рекламирања послова на Интернету, искоришћавања лица која су се са извршиоцем упустила у романтичну везу преко Интернета, до лица која су свесна своје улоге и новац и робу свесно прослеђују уз одређени проценат. Врло често се користе и методе социјалног инжињеринга како би се лица довела у заблуду да раде легалан посао.[3]

Извршиоци кривичних дела користе на Интернету *Chat room* опције, социјалне мреже, лажне рекламе и лажне профиле како би пронашли и

[1] Аналогија са мулама за дрогу. У питању је алузија на давно коришћене животиње за пренос терета које су, у ствари, представљале средства за рад која су заменљива и потрошна, у која се мало улаже а имају велику употребну вредност. Више о овоме на http://en.wikipedia.org/wiki/Money_mule датум посете: 31.12.2009.год.

[2] Према http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf датум посете: 15.12.2009, постоје више врста ових облика превара а неке које су биле најактуелније 2008. и 2009.год. су: превара кућних љубимаца, прикривених купаца (или превара трансфера средстава), цимерске преваре, превара усвојења (преваре у добротворне сврхе), романтичне преваре, преваре које укључују логое и обележја ФБИ, превара прекомерне исплате, онлајн аукцијске преваре, превара лажних акредитива (escrow service) и друге.

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

ангажовали лица за криминалне активности, и како би их убедили да у тим активностима учествују. Такође, веома често користе и податке и контакте које су корисници сами оставили на Интернету приликом објављивања биографија за посао, евентуално личних сајтова или сајтова привредних друштава органа и организација чији су радници (а које оне објављују). Поред ангажовања лица преко Интернета извршиоци кривичних дела из области високотехнолошког криминала користе и лица из своје непосредне околине како би за њих подигли новац или робу, најчешће, уз одређену надокнаду.

У току 2008. и 2009. године на територији Републике Србије откривено је да су извршиоци кривичних дела из области високотехнолошког криминала по наведеном принципу ангажовали више лица за пријем и подизање робе и новца који је противправно прибављен извршењем кривичних дела рачунарске преваре и злоупотреба платних картица на Интернету.

II. НАЧИН АНГАЖОВАЊА ЛИЦА

Начини ангажовања лица за подизање новца и робе релативно су једноставни. Врло често се користе варијанте рекламирања одређених послова на Интернету или се директно контактирају лица која траже посао преко Интернета. Такође се користе и шеме у којима се лица ангажују на емотивној основи тзв. романтичне шеме. Такође се користе и шеме са прикупљањем добротворних прилога у којима се жртва преваре убеђује да ради користан хуманитарни посао на тај начин што обезбеђује да се на његов рачун уплаћује новац у одређену хуманитарну сврху, а потом тај новац даље пребацује, не знајући прави разлог, извршиоцима кривичних дела. На тај начин извршилац кривичног дела задобија поверење жртве која му помаже да новац прикупљен преварама добије назад као легалан, а што и представља веома чест modus operandi оваквих извршилаца. Веома је значајно припремити или искористити моменат задобијања поверења, круцијалан је моменат довести жртву у жељено стање и искористити предност. Понекад се дешава да се круг лица шири и са члановима фамилије жртве[4] која их је убедила да чини добру и корисну ствар, тако да и они постају жртве несвесне

[4] Ово је посебна специфичност социјалног инжењеринга, уколико извршилац (преварант) буде значајно убедљив може постићи веома квалитетне резултате, јер тада жртва постаје продужено оружје (наравно изманипулисано) и онда превара добија своју праву димензију, превара сама себе одржава.

својих поступака, тј. несвесне да у ствари помажу извршиоцу кривичног дела да врши прање новца. [5]

Како би избегли знакове упозорења система за спречавање превара које банке поседују рачуни ангажованих лица користе се у одређеном временском интервалу и новац се пребацује у тачно одређеној суми и по одређеној количини трансакција. Банке врше надзор (мониторинг) већих трансакција па се новац на рачуне ангажованих лица пребацује у мањим количинама како би се избегло откривање сумњивих трансакција[6].

Извршиоци кривичних дела врло често путем Интернета објављују рекламе за посао „финансијског агента". Након тога траже лица која су погодна да отворе рачун или дозволе приступ банковном рачуну у њиховој држави. Потом, извршиоци врше трансфер новца или робе прибављене путем Интернета на рачун лица које се пријавило за посао. Преко свог рачуна лице шаље новац назад извршиоцу кривичног дела, а задржава одређени, унапред договорени износ као провизију.

А. Преваре типа: „кућна радионица" (work-at-home scams)

Преваре овог типа врше се на тај начин што извршиоци кривичних дела ангажују лица преко фиктивних *On line* компанија које изгледају као легалне, или преко *spam*[7] порука којима се нуди наводно запослење путем електронских порука. Врло често се за овакве послове дају звучна имена помоћу којих се код лица ствара утисак да се ради о сасвим легалним пословима као што су: 'Private Financial Receiver', 'Money Transfer Agent', 'Shipping Manager' и 'Sales Representative'.[8] Овакве поруке сличне су фишинг порукама, али је разлика у томе што се код ових порука жели постићи потпуна контрола над рачуном ангажованог лица, као и његов пристанак да учини оно што се од њега тражи, тј., да врати назад новац који му је од стране извршиоца уплаћен на рачун. Врло честе преваре овог типа су „work-at-home scams" преваре у којима се лицима примаоцима поруке нуди да посао раде од куће уз одређени проценат. За ове поруке се користе

[5] Abbay&Loyd: *Fighting back against Online Fraud, Risk Management,* Article No.2, UK, p. 2 http://ezinearticles.com/?Fighting-Back-Against-Online-Fraud&id=3392818, датум посете: 21.01.2010. године.

[6] Finjan Malicious Code Research Center: *Cybercriminals use Trojans & money mules to rob online banking accounts*, Cybercrime Inteliigence Report Issue No.3, USA, Orange, 2009, 6.

имена звучних предузећа. Даљи кредибилитет се остварује тиме што лица учествују у попуњавању различитих формулара, шаљу CV и сл, као да се ради о легалном послу. Ове преваре су нарочито учестале прошле године на адресе наших корисника у Србији.

Б. Преваре са преусмеравањем поштанских пошиљки (Reshipping)

Ова варијанта ангажовања лица за прибављање робе веома се често користи од стране извршилаца кривичних дела из области високотехнолошког криминала. Ангажовано лице прима поштанску пошиљку на своју кућну адресу (у пошиљци се налази илегално прибављена роба) и потом је поново шаље извршиоцу кривичног дела, у замену за одређену надокнаду по сваком прослеђеном пакету.

Овакви договори се праве најчешће тако да новац стиже директно на рачун ангажованог лица. Након тога ова лица могу да се ангажују и за даљи трансфер новца преко њиховог рачуна. Овај облик прибављања противправне имовинске користи веома је чест, посебно због брзог трансфера новца, популарности *On line* трговине, профитабилности и претпоставке да је куповина преко Интернета веома честа и да пошиљке нису изложене интензивној контроли, тежњи продаваца да скупу робу продају широм света, ограничене контроле пошиљки које се шаљу од стране различитих лица са различитих меридијана.

Најчешће се шаљу лап топови, *PDA* уређаји, мобилни телефони и сл (у питању су ствари обично, релативно веће вредности, а којима се теже улази у траг). Ова роба најчешће је купљена из украдених фондова извршилаца кривичних дела.

Како би привукли што више лица извршиоци кривичних дела користе услуге великих компанија као што су Monster.com и CareerBuilder.com како би,

[7] Spam представља један од облика нежељене и незахтеване електронске поште, или комерцијалних порука, често упућених већем броју лица. За више о овоме погледати у **S**.C.McQuade, Encyclopedia of cybercrime 2009. Greenwood Press, 88 Post Road West, Westport, pp 169-170. И не тако давно, (још 1998.год.) се у парламенту САД водила полемика о карактеристикама и облицима спречавања овог облика нежељене поште. Више о овоме на: http://www.legi-internet.ro/spamsen.htm датум посете: 01.01.2010.год. Иначе се реч спам користи већ неких 70 година. У поменутој енциклопедији се наводи да је термин први пут коришћен 1937.год.

[8] The Australian High Tech Crime Centre, *Money mules, Australian Institute of Criminology*, Australia, 2007, 17.

под фиктивним фирмама, прикупљали податке о лицима која би се могла ангажовати у ове сврхе, (data mining for victims, копање по подацима у потрази зха жртвама). Иако ове компаније врше надзор реклама које се код њих објављују, због саме природе Интернета, јако је тешко открити која фирма се бави оваквим активностима, пошто се оне сваког дана гасе, а појављују нове.

В. Преваре на основу романси (Romance scames)

На Интернету постоји много Интернет сајтова и сервиса који пружају могућност за упознавање, дружење и забављање. Многи корисници Интернета користе услуге ових сервиса за упознавање потенцијалних партнера. Извршиоци кривичних дела све чешће користе усамљеност[9] ових корисника и нуде им различите романсе преко Интернета, упознајући их, задобијајући њихово поверење и припремајући се за извршење кривичних дела месецима. Овакви извршиоци се труде да уђу у психу жртава и одржавају параноидну конструкцију која храни сујету и искоришћава слабости жртава, све у циљу максималног искоришћавања жртве. Најчешће облике превара које се врше на овај начин су тражење новчане помоћи за авионску карту како би дошли на састанак и на „коначно“ упознавање, тражење помоћи за наводно болесног рођака и др. [10]

Романтичне преваре[11] за предмет напада имају особе које користе мреже за сударе на слепо и социјалне мреже. Након контакта овим путем преварант тежи задобијању поверења жртве кроз различите облике изјава о наклоности или изливима љубави, често преваранти живе далеко од жртве (у већини случајева у другој земљи), након чега преварант изражава незадрживу жељу да се са жртвом физички сретне. Уколико жртва пристане онда креће игра – преварант нема довољно новца да допутује на место које је договорено за сусрет и захтева од жртве да пошаље новац како би могао да допутује да би се видели. Након пријема

[9] Сами фактори који наводе људе на онлајн састанке и остваривање социјалних и љубавних контаката на нету су, у ствари, исти фактори који их и чине веома рањивим на нападе социјалног инжењеринга, а то су: 1. Јака жеља и потреба за новом везом, 2. Природна тенденција већине да се негде појаве и да примете и буду примећени и 3. Потреба да размене личне податке и информације са потпуним странцима.

[10] Australian Bankers Assotiation Inc and Australian Federal Police, *Fact Sheet: Warning to students – don't get caught by mule scams*, http://www.afp.gov.au/__data/assets/pdf_file/130791/MR_091012_Warning_student_mule_job_scam_Fact_Sheet.pdf , датум посете 10.01.2009.

[11] Погледати на http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf, датум посете: 15.12.2009

новца превара се развија на различите начине, тада се дају најразличитија објашњења типа преварант је због плејаде непредвидивих догађаја у међувремену (или чешће у току путовања, услед, на пример несреће на путу) напрасно упућен у болницу и неопходно је да се покрију трошкови лечења, брат преваранта је отет па је неопходно да се прикупе средства за ослобађање и сл. У свакој даљој секвенци догађаја преварант тражи још новца док жртва не пресуши или престане да верује обмани.

Овакве шеме често се користе и да се омогући пребацивање новца, преусмеравање пошиљки преко жртве преваре и сл.

III. ИСКУСТВА МУП-а РЕПУБЛИКЕ СРБИЈЕ У ОТКРИВАЊУ ПОСРЕДНИКА

Извршиоци кривичних дела из области високотехнолошког криминала на територији Републике Србије углавном су лица по овом принципу ангажовали за пријем и подизање робе и новца који је противправно прибављен извршењем кривичних дела рачунарске преваре и фалсификовање и злоупотреба платних картица која су вршена на Интернету.

У току 2008. и 2009. године на територији Републике Србије откривено је десет случајева рачунарских превара и злоупотреба платних картица извршених на Интернету, у оквиру којих су покушане и извршене злоупотребе података са више платних картица, а прибављена имовинска корист износила је преко пет милиона динара. Идентификовано је дванест лица која су се бавила овим кривичним делима и против њих су поднете кривичне пријаве. Злоупотребљаване су, углавном, платне картице страних банака са територије Сједињених Америчких Држава, а за прибављање података коришћене су технике *SPAM*-а, *phishing*-а и *SQL* инјекција[12]. Приликом вршења ових кривичних дела извршиоци су ангажовали лица која су, за одређену новчану надокнаду и надокнаду у роби, преузимала робу и новац за рачун извршилаца.

У највећем броју случајева радило се о ангажовању лица по принципу преузимања и преусмеравања поштанских пошиљки. У наведеним случајевима електронски подаци са платних картица добијени извршењем кривичних дела преко Интернета најчешће су коришћени за наручивање робе преко Интернет

[12] Подаци присутни у овом делу текста прибављени су из праксе једног од аутора.

сајтова електронских продавница, најчешће на територији Републике Србије, али и у иностранству. Извршиоци кривичних дела су, на основу досадашњих искустава, углавном била малолетна лица или млађи пунолетници, док су се као саизвршиоци појавила и старија пунолетна лица која за одређену надокнаду, под лажним идентитетом, преузимају наручену робу.

Извршиоци кривичних дела углавном су наручивали скупоцену робу (мобилне телефоне, лап топ рачунаре, злато, аудио и видео технику и др) коју након извршења кривичног дела могу лако и брзо да препродају. Приликом наручивања робе извршиоци утичу на процес обраде података тако што уносе податке о платним картицама у поља за унос података на Интернет сајту електронске продавнице, и дају лажне личне податке (име, презиме, адресу) представљајући се као да су они власници платне картице, а за евентуалне договоре око преузимања робе остављају бројеве мобилних телефона намењене само за ту сврху (најчешће мобилне телефоне лица која су ангажовали за преузимање пошиљке). Како би остали анонимни, као контакт електронску адресу остављају електронске адресе отворене на Интернет сервисима који омогућавају *Web* базирану пошту, где је тешко добити податке о власницима, јер се сервери налазе у иностранству (нпр. *Gmail*)[13], као и контакте лица која ће робу примити на своју адресу. При наручивању робе остављају и фиктивне податке ради преузимања робе на отвореном простору испред адресе коју дају као место за контакт и испоруку. [14]

Пошто се испорука робе често врши путем поште, теренском доставом, за примаоце робе се бирају лица која су пунолетна и поседују личне карте. Ова лица, најчешће под лажним именом и презименом, на отвореном простору, робу преузимају директно од доносиоца, након телефонског позива од стране достављача, како би избегли да буду откривени и ухваћени од стране полиције и како би се избегло да се сазнају праве адресе испоруке пошиљака. Лица која преузимају робу најчешће нису и лица која су робу наручивала преко Интернета, већ раде за одређени проценат од продаје робе која је на овакав начин прибављена.

[13] Наравно анонимност је обезбедио неки од ових веб сервиса, у сваком случају, јер је веома лако остварити отварање мејл налога, без давања неких посебних додатних информација о власнику, шта више, могу се давати и лажна имена и лажне мејл адресе, и тиме прикрити траг до лица које је власник.

[14] В. Урошевић, *Злоупотребе платних картица и рачунарске преваре*, Правни информатор бр. 9, Београд, 2009, 6.

Код кривичних дела рачунарских превара и злоупотреба платних картица извршених на Интернету коришћење лажног идентитета повезано је са коришћењем туђих идентификационих података, или тотално измишљеним подацима.

Прикривање идентитета врши се на много различитих начина, а већина случајева прикривања везана је за сакривање идентитета наручиоца робе и лица које је злоупотребило платну картицу при вршењу рачунарске преваре. Извршиоци кривичних дела у овим случајевима користили су (услуге) лица која су ангажовали за преузимање робе како би прикрила свој идентитет.

Након идентификације локације са којих је наручивана роба тј. одакле је извршена рачунарска превара и злоупотреба платних картица, као и извршилаца ових кривичних дела а по прибављању наредбе дежурног истражног судије, вршени су претреси станова и других просторија осумњичених лица. Идентитет лица која су преузела робу утврђен је након преузимања робе.

У једном од наведених случајева је дошло и до тзв. „Преваре на основу романсе“. Страни држављанин, мушког пола, је, путем једне од социјалних мрежа, преко Интернета контактирао држављанку Републике Србије. Након више месеци дописивања и упознавања замолио је да му да адресу пребивалишта, фиксни телефон и своје податке како би за њега примила робу (компјутерске компоненте), пошто он није у могућности да пошиљку прими у својој држави. Описане чињенице су, социјалним инжењерингом, веома перфидно упаковане у друге облике удварања тако да жртва има веома мало маневарског простора и избора уопште. Роба је купљена преко Интернета у једној електронској продавници са подручја Републике Србије. Након испоруке пошиљке и утврђивања идентитета лица које је преузело робу, прегледом њеног профила на социјалној мрежи[15], утврђено је да се лице са којим је контактирала заиста налази у иностранству. Приликом обављања разговора она је навела да је пристала да робу преузме на своје име зато што јој је извршилац био симпатичан, да није сумњала да се ради о превари, обзиром да јој се извршилац представио као директор у једној успешној иностраној фирми и сл. Приликом упознавања по њу је дошао возилом неке стране фирме. Жртва, у овом случају[16], није имала одговор

[15] За чије коришћење и претраге је она добровољно дала дозволу припадницима полиције.
[16] Жртва у смислу социјалног инжењеринга, али у случају превара са картицама или рачунарских превара се може, условно, сматрати саучесницом.

у погледу детаљнијих података о лицу као што су име, презиме и сл. На описани начин методом социјалног инжињеринга искоришћено је поверење особе женског пола и на основу, вештачки диригованог и креираног, емоционалног односа ово лице је наведено да преузме робу за рачун извршиоца кривичног дела.

Извршиоци кривичног дела су, у једном од ових случајева, ангажовали лице које је отварало рачуне у банкама на територији Републике Србије и потом подизало новац који су жртве кривичних дела рачунарске преваре, злоупотребе и фалсификовања платних картица уплаћивале на његов рачун, по инструкцијама извршилаца кривичних дела. Након уплата од стране оштећених, лице је уз одређену провизију подизало овај новац и предавало га извршиоцима кривичних дела.

IV. ЗАКЉУЧАК

Ангажовање посредника за подизање новца и робе противправно прибављених извршењем кривичних дела из области високотехнолошког криминала преко Интернет сајтова на којима се нуди запослење и/или путем *spam* порука представља кључни пример нових напада криминалаца и криминалних група који нису усмерени на компјутерске системе (синтактички) већ на њихове кориснике (семантички). У многим државама лица пристају на оваква ангажовања из очајничке жеље да нађу запослење, па врло често не постављају никаква питања. Главни проблем са овом појавом је чињеница да лица ангажована у овим активностима, условно[17], могу да одговарају за саучесништво при извршењу кривичних дела, па и да одговарају за кривично дело прања новца.

Како би избегли да постану жртве кривичних дела или саучесници врло је важно упозорити кориснике Интернета да се у порукама овакве садржине на Интернету могу открити и потенцијални знаци да се ради о покушају ангажовања у описане сврхе. Неки од ових индикатора су[18]:

[17] Кривично правно посматрано у овим случајевима акцесорна природа саучеснишва виси о веома танкој нити и може се спекулисати о постојању свести о противправности радње, тако да можемо говорити о одговорности али, наравно, постоје и друга мишљења.

[18] Листа ФТЦ (Federal trade commision) од класичних 12 превара (алузија на 12 жигосаних, према Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection) садржи:
- лажне пословне прилике
- ланчана писма
- преваре са радом у кући
- здравствене и дијететске преваре
- лаке прилике за зараду

- Од компаније која нуди посао стигла је порука са информацијом да се уплате могу вршити директним депозитом. У поруци се од примаоца поруке тражи да проследи податке о свом личном банковном рачуну.

- Наводна пословна организација која нуди запослење комуникацију остварује преко бесплатних Интернет сервиса за електронску пошту као што су *Yahoo*-а или *Hotmail*-а.

- Граматичке и друге грешке у порукама које стижу.

- Провере преко *Whois* сервиса у вези домена компаније који се користи указују на неслагање између државе у којој је хостован домен Интернет странице праве компаније и лажне странице која је постављена од стране извршилаца кривичног дела[19].

Препоруке многих полицијских и других служби широм света су да поруке са овим садржајем треба одмах обрисати, а да *On line* контакте који се нуде од стране непознатих лица преко Интернет сервиса треба игнорисати. Основна „парола“ везана за ове врсте ангажовања у рекламним кампањама државних органа широм света су: „Ако Вам неко понуди да на лак начин зарадите новац, и понуда вам се учини сувише невероватном да би била истинита, онда она то вероватно и није!“

Уколико испоштују све савети и препоруке крајњи корисници могу да избегну ситуације у којима могу да постану жртве оваквих пословних понуда. То могу да учине једино ако воде рачуна да неприхватају понуде којима им се предлаже да само примају новац и врше његов даљи трансфер преко рачуна. Посебно треба да воде рачуна о томе да приликом читања електронских порука не

- бесплатна роба
- прилике за инвестиције
- преварне масовне електронске поруке
- пакети за дескрембловање кабловске телевизије
- гарантовани кредити или зајмови
- промотивне понуде наградних путовања
- преваре у вези побољшања кредитних способности

[19] Постоје категорије превара електронском поштом које се могу превентирати следећима активностима:
- филтрирањем спама
- немојте веровати непознатим електронским порукама
- односите се према сумњивим порукама са дужном пажњом и опрезим
- немојте кликтакти мишем на линкове у електронским порукама
- инсталирајте антивирусне и фајервол програме и ажурирајте их редовно
- конфигуришите свој клијент електронске поште безбедно

посећују Интернет линкове који се користе као референца одређене компаније, пошто се извршиоци кривичних дела служе овом могућношћу да методом социјалног инжињеринга наведу лице да посети Интернет страницу коју су сами креирали да би их убедили да се заиста ради о легитимним компанијама, њиховим правим представнивцима и сл. Најбоље би било да корисник изврши независну претрагу везану за провере компаније која нуди посао, као што је нпр. слање електронске поруке на праву адресу компаније, провера домена и сл. Податке о свом рачуну и идентификационе податке не треба давати никоме. Новац никада не треба слати лицима као помоћ, посебно ако се ради о електронском трансферу новца. Своје финансијско стање, новчана примања и сл. не треба саопштавати на Интернету. Посебно треба поставити и питање зашто за пословну понуду није обављен интервју, зашто би неко поверавао свој новац лицу које не познаје, зашто било коме требају подаци о нашем банковном рачуну итд.

Чињеница је да овај феномен код нас није довољно познат широј јавности и корисницима Интернета, посебно зато што та тема није довољно заступљена у медијима. Превентивно деловање државних органа као што су полиција и тужилаштво има кључну улогу када је спречавање ове појаве у питању. Потребно је што хитније деловати проактивно, искористити потенцијал медија и скренути пажњу домаћој јавности на финансијске губитке који настају као последица ових криминалних активности. Превентивна улога полиције у заштити корисника Интернета са територије Републике Србије од оваквим активностима сигурно би била успешнија и сврсисходнија од репресивних активности које се предузимају након сазнања да је кривично дело извршено.

Vladimir Urošević – Zvonimir Ivanović

THE ROLE OF INTERNET IN HIRING A THIRD PARTY TO TAKE OVER GOODS AND MONEY UNLAWFULLY ACQUIRED BY COMMITTING HIGH TECHNOLOGY CRIMES

Summary

Hiring a third party to raise goods and money unlawfully acquired by committing crimes in the field of high technology criminality, has become a global widespread phenomenon with the appearance of internet. During crime-solving and

locating of those persons, the larger number of them cannot give valid information (and sometimes any information at all) on a true perpetrator. In hiring individuals for this role, crime perpetrators use various methods and often they use methods of social engineering to make those individuals believe they were doing legal business. The perpetrators of those crimes use chat room options on the internet, social networks, false advertisements and profiles. They also use information and contact addresses that users left on the internet by themselves sending their biographies to apply for a job, web sites with possible personal contents or information from the web sites of their employing companies, institutions and other organizations (official web sites). The ways of hiring persons to take over goods and money varied a lot, as well as the forms of frauds, enabling full creativity of perpetrators in such cases. In this work, the authors point out to different patterns and methods used by the Serbian police and give broader analysis of perpetrators modus operandi and the way they approach to victims getting them into their net showing large diapason of fraud possibilities available to every perpetrator. The authors give us broader accounts of following types of frauds: work-at-home scams, fraud with redirecting of mails (Reshipping), fraud based on romance (Romance scams). After an overview on the mentioned types of frauds, it is given recapitulation of Serbian Ministry of Interior Affairs current experience in combating high technology crimes with the statistics from last two years. Analysis has been carried out through portraying perpetrators, victims (or hired third parties exploited for the crime), means and ways to commit the crime. The special attention is paid to one case from the practice concerning romance scams. On this example, the group of similar cases can be analyzed very well making important conclusions and the authors do that.

Key words: computer fraud, credit card fraud, "money mules", social engineering.