

КРИМИНАЛ У УСЛОВИМА ПРИМЈЕНЕ ИНФОРМАЦИОНЕ ТЕХНОЛОГИЈЕ

Милица Тепшић,

Министарство управе и локалне самоуправе
Бања Лука, Трг Републике Српске 1
m.tepsic@mul.svladars.net

II

Младен Радивојевић,

Министарство управе и локалне самоуправе
Бања Лука, Трг Републике Српске 1
m.radivojevic@mul.svladars.net

Лејла Решић,

Министарство управе и локалне самоуправе
Бања Лука, Трг Републике Српске 1
l.resic@mul.svladars.net

Сажетак: У овом раду описани су нови облици злоупотреба и превара изазвани брзим развојем информационе технологије, која је постала стуб на коме савремено друштво заснива своју садашњост и гради своју будућност. С развојем информационог друштва, злоупотреба информационе технологије постаје све чешћа, а по посљедицама све опаснија. Заштита од рачунарског криминала постаје важна функција друштва, јер се са сваком технолошком иновацијом јављају нове злоупотребе почињене на рачунарима или уз њихову помоћ. Сусрећу се на свим локалним и регионалним нивоима, а испреплитањем рачунарских мрежа и експанзијом Интернета и на свјетским просторима.

Кључне ријечи: рачунарски криминал, злоупотреба, информационе технологије

Abstract: *In this work we described new forms of abuse and fraud caused by fast development of information technology, that became a foundation for modern society to base its present and to built its future. With the development of information society, the abuse of information technology becomes more common, and the consequences of increasingly dangerous. Protection against cyber crime is becoming an important function of society, because with each new technological innovation occurring abuses committed on computers or with their help. They meet at all local and regional levels, and interweaving of computer networks and expansion of the Internet and the global spaces.*

Keywords: *computer crime, abuse, information technology*

1. УВОД

Криминал постоји од давнина, а данас добија нове облике и ново окружење. Са развојем рачунарске технологије постаје глобалан, бришући разлике између земаља, подручја, континента.

Рачунари у раним фазама њиховог развоја нису баш били погодни за неке веће злоупотребе због тога што је њихово коришћење подразумијевало специјалистичко образовање, тако да се њима бавио само релативно узак круг информатичких

стручњака, и због тога што се они раније нису налазили у масовној употреби. Током посљедње двије деценије, рачунарска индустрија је доживјела велику трансформацију од "затворених" мрежа оформљених око централних рачунара до "отворених" мрежа које користе Интернет¹. Значај Интернета је у томе што поред лакоће коришћења, допушта интеракцију корисника, знатно убрзава трансакције, штеди вријеме и омогућава приступ информацијама 24 часа, седам дана у недјељи, 365 дана у години. Можда најбитнија карактеристика Интернета је што се непрестано развија, расте и прима нове кориснике, па повезивањем на Интернет, постајете члан заједнице корисника једног огромног система, који превазилази значај појединца и у коме вријеме и простор готово ништа не значе.

Технологија и рачунари омогућавају нам једноставнији и ефикаснији живот, али при томе и прилике за злоупотребу, као и опасности од злонамјерних корисника. Брз развој информационих технологија и бројне промјене које оне са собом доносе, погодују криминалним активностима и чак подстичу њихово настајање, ширење и интензитет. Могуће негативне посљедице произилазе из чињенице да се све више вриједних друштвених добара (новац, роба, подаци и сл.) претвара у "пакете" и смјешта у рачунарске системе, а познато је да криминалци увијек крећу ка мјестима гдје се такве вриједности налазе. Криминалци су одавно уочили да су идеална поља за криминалну дјелатност области у којима се појављују нове технологије и идеално вријеме прије него што је друштво у тој области успјело да изгради и развије адекватне системе заштите.

2. ПОЈАМ И ДЕФИНИСАЊЕ РАЧУНАРСКОГ КРИМИНАЛА

„Рачунарски криминал је општи појам који обухвата кривична дјела која се врше посредством рачунарског система или мреже, у рачунарском систему или мрежи, или против рачунарског система или мреже. У принципу он укључује било које кривично дјело које се врши у дигиталном амбијенту.“²

Поред дефиниције формулисана од стране УН и друге међународне организације и појединци бавили су се дефинисањем појма рачунарског криминала. Из тога се најбоље може закључити колики се значај придаје изучавању ове врсте криминала широм свијета.

Дефиниција усвојена од стране *OECD* гласи: „Криминал повезан са рачунаром је свако илегално, неетичко или неовлашћено понашање које укључује аутоматску обраду података или пренос података“.

У теорији кривичног права могу се наћи и многобројне дефиниције рачунарског криминала формулисана од стране појединаца. У ту групу дефиниција спадају појмовна одређења рачунарског криминала Дона Паркера, Августа Бекваја, Бого Брвара, Ђорђа Игњатовића и Слободана Р. Петровића.

У свијету се користе многи термини који означавају ову појаву – *computer abuse*, *computer fraud*, *crime by computer*, технокриминал или рачунарски криминал.

Рачунарски криминал је противправна повреда имовине код које се рачунарски подаци с предумишљајем мијењају (манипулација рачунара), разарају (рачунарска

¹ Према саопштењу Агенције Уједињених нација - Међународна унија за телекомуникације (*ITU*) број корисника Интернета у протеклих пет година се удвостручио, а од 226 милиона нових корисника у 2010. години 162 милиона је из држава у развоју, гдје су стопе раста више.

² United Nations year 2000 Crime Congress, *Background paper for the workshop on crimes related to the computer network*, према Бановић Б., оп. цит. стр. 132.

саботажа), до њих се неовлаштено долази и користи (рачунарска шпијунажа) или се користе заједно са хардвером (крађа времена).

Као свеобухватну функционалну дефиницију, могли бисмо да прихватимо ону која рачунарски криминал дефинише као радњу која се предузима уз употребу рачунара и других средстава информационих технологија, а која је усмјерена на:

- неовлашћени приступ заштићеном рачунару
- неовлашћено пресретање електронских података који су упућени са рачунара или ка другом рачунару
- уништавање, измјену и брисање електронских података
- ометање или онемогућавање функционисања рачунарског система путем оштећења, брисања, мијењања или уметања електронских података
- дистрибуцију недозвољених садржаја
- стварање и ширење вируса и малициозног софтвера.

У односу на чињеницу да ли се рачунар, систем или мрежа користе као средство за извршење дјела или су објекат на коме се дјело извршава, понекад се користе различити изрази да би се дефинисала криминална дјелатност која се врши употребом рачунара:

- класичан рачунарски криминал код кога је рачунар или рачунарски систем средство извршења или објекат напада;
- Интернет криминал код кога је злоупотреба мреже одређујући фактор (посједовање и дистрибуција дјечије порнографије, распиривање националне и расне мржње, неовлашћена дистрибуција ауторских дјела и предмета интелектуалне својине);
- е-криминал који се везује за злоупотребу комуникационих уређаја и уређаја за складиштење електронских података

3. ЗЛОУПОТРЕБЕ И ПРЕВАРЕ ПРИМЈЕНОМ НОВИХ ТЕХНОЛОГИЈА

Нове технологије пружају велике могућности за различите врсте злоупотреба и превара, највише из разлога што механизми заштите пословања на Интернету још увијек нису довољно развијени. Данас многи преваранти користе Интернет за различите врсте злоупотреба и превара. Према истраживању америчког удружења за заштиту потрошача (*NLC*)¹, чак 98% испитаних је рекло да су бар једном добили *e-mail* у којем су им биле понуђене финансијске услуге или необични пословни приједлози.

Преваре чини скуп активности које карактеришу обмана, лажно представљање, прикривање чињеница, манипулација, изгубљено повјерење и слично. Ова категорија је позната и под називом "криминал бијеле крагне". Основно обиљежје овог дјела је довођење неког у заблуду да би се тиме прибавила противправна имовинска корист. У суштини се свде на лажно приказивање чињеница или прећуткивање чињеница. Аутоматизацијом класичних и настајањем нових метода овај вид злоупотреба добија и на квалитету и на квантитету.

Један од најраспрострањенијих облика кривичних дјела преваре који се врши уз помоћ рачунара је превара позната као „Нигеријска превара“² или „Превара 419“.

¹ *NLC - National Consumers League*

² „Нигеријска превара“, или превара позната под називом „превара 419“, појавила се раних 80-тих година, са наглим економским развојем Републике Нигерије, који се заснивао на употреби нафтних ресурса. У току прве деценије 21-ог вијека „превара 419“ постала је веома популаран начин извршења кривичних дјела преваре у Африци, Азији и Источној Европи, а у последње вријеме и у Сјеверној Америци, Западној Европи (углавном Великој Британији) и Аустралији.

Добила је назив по члану број 419 Нигеријског кривичног закона (који је дио поглавља 38) под називом „Прибављање имовине помоћу преварних радњи: Превара“, који дефинише ово кривично дјело (Chawki, 2009:2). Америчко друштво за дијалектику је утврдило да се израз „превара 419“ користи од 1992. године. „Нигеријска превара“ је метода вршења кривичног дјела преваре уз помоћ рачунара и најчешће почиње писмом или електронском поруком која је тако осмишљена да изгледа као да је намјерно послата примаоцу поруке. Радња извршења „Нигеријске преваре“ углавном почиње убјеђивањем „жртве“ преваре да учествује у подјели одређених новчаних фондова ако унапријед уплати одређени новчани износ који је, у највећем броју случајева, неупоредиво мањи од оног износа који би требало да добије као корист од тог фонда (Smith et al., 1999:1).

Вријеме свјетске кризе показало се као одлично вријеме за Интернет преваре. *Cyber* криминалци постали су софистициранији и технолошки напреднији, па према извјештају специјализоване компаније за *online* безбједност *Actimize*, представљено је десет најчешћих начина за преваре путем Интернета:

- Преваре на друштвеним мрежама - криминалци хакују (неовлашћено преузму, "уђу") на налог корисника на некој од *online* друштвених мрежа, као што су *Facebook*, *Twitter*, *MySpace* или *Bebo* и шаљу поруке пријатељима и члановима породице да су у невољи и да је потребно одмах да се пошаље новац на неку адресу.
- "Кладионичарска" превара - жртва добија резултат фудбалске утакмице путем електронске поште. Трик је у томе што већина корисника која прима овакве поруке добија нетачне резултате, али ипак мањи проценат корисника добија и тачне резултате.
- Преваре "уштеде новца" - савршене за периоде економских криза, ове преваре путем Интернета, телефона или поште укључују велики број финансијских помоћи и понуда за консолидацију кредита и кредита за некретнине, снижење каматне стопе, и сл., уз обавезу корисника да уплати одређени износ.
- "Црна" превара - углавном се виђа у Азији, није тако честа на Западу. Наиме, преваранти обично позивају или шаљу *e-mail* старијој особи наводећи да је њихово дијете страдало у саобраћајној несрећи и да је потребно хитно да уплате одређени новчани износ.
- Понуда коју не можете одбити - корисницима Интернета нуде се чекови, најчешће украдени као награда за куповину неког производа. Такође, тражи се од купаца да уплати депозит на неки рачун, уз неку провизију коју задржава жртва преваре. Међутим, чек се убрзо сторнира, док криминалци узимају депозит.
- Неауторизована компанија (*e-processor*) за наплату - корисницима се шаљу захтјеви за "поновним уписом корисничких информација о броју платне картице", у оквиру чега су странице идентичне страницама неких познатих компанија, као што су *eBay*, *Amazon* и сл., само је адреса потпуно различита.
- Телефонска превара - преварант позива корисника и информише га да је дошло до проблема са сигурношћу у оквиру његовог налога. Затим путем конференцијске везе криминалац позива банку, чији представник тражи сигурносне информације (лозинку и тајно питање, или ПИН code). Жртва одговара на питања о тајним подацима и на тај начин и преварант долази до неопходних информација да покраде новац са рачуна.
- *E-mail* са "тројанцима" - када корисник у оквиру *e-maila* кликне на линк, или отвори прилог поруке, уколико нема ефикасну Интернет заштиту, заразиће се тројанцем, злоћудним програмерским кодом који ће са рачунара покрасти све тајне податке и шифре.

- Лажни *Escrow* сервис - ово се дешава само корисницима *Escrow* сервиса компаније *eBay* који омогућава сигурну наплату између корисника.
- "Пецароши" - криминалци се представљају као легитимне организације, најчешће у форми електронске поште које траже сигурносне податке или *PayPal* тајне шифре, податке за приступ *online* рачуну у банци, лозинке или детаље за пријављивање¹.

4. ЗАКЉУЧАК

Рачунар представља једну од најзначајнијих и најреволуционарнијих тековина развоја техничко–технолошке цивилизације. Но, поред свих предности које собом носи и огромне користи човечанству, рачунар је брзо постао и средство злоупотребе несавјесних појединаца, група чак и организација. Тако настаје рачунарски криминалитет као посебан и специфичан облик савременог криминалитета по структури, обиму и особеностима. Све то заслужује пажњу државе и њених органа па и цијеле међународне заједнице, јер злоупотреба информационо-комуникационих технологија представља реалност која се не смије игнорисати.

Управо због тога безбједносна компонента никако не би смјела бити запостављена, а она подразумијева предузимање превентивних мјера, које би морале бити подржане и репресивним мјерама. Дугорочно гледано, ово би била најкориснија и најисплативија инвестиција у информациону будућност.

5. ЛИТЕРАТУРА

- [1.] Алексић Ж. Миловановић З., *Лексикон криминалистике*, Београд, 1993.
- [2.] Computer Crime and Intellectual Property Section (CCIPS), www.cybercrime.gov/Osowski_TangSent.htm, Novembar, 2001.
- [3.] Chawki, M., (2009), 3. *Nigeria Tackles Advance Fee Fraud*, *Journal of Information, Law & Technology*, University of Warwick, Great Britain, (1), стр.1-20
- [4.] Дракулић М., *Основи компјутерског права*, Београд, 1996.
- [5.] Jack Karp, *Get Help Fighting Fraud Online*, Мај 2002.
- [6.] Kerry & Linda McNeil, *Internet Frauds and Risks*, New York Cash Exchange доступно на: www.phoenixhecht.com/PDF/InternetFraud.pdf, 2000.
- [7.] Krauss L., Mac Gahan A., *Computer Fraud and Countermeasures*, New Yersey, 1979.
- [8.] Smith, R., Holmes, M., Kaufmann, P., (1999), 6. *Nigerian Advance Fee Fraud, Trends and Issues in crime and criminal justice*, Australian Institute of Criminology, Australia, стр. 1.
- [9.] United Nations year 2000 Crime Congress, *Background paper for the workshop on crimes related to the computer network*, према Бановић Б., оп. цит. стр. 132.

¹ *Economy.rs, Times Online* 10. август 2009