Prof. dr. sc. Slavko Šimundić,
redoviti profesor u trajnom zvanju Pravnog fakulteta u Splitu

Siniša Franjić,
asistent na Elektrotehničkom fakultetu u Osijeku

Krešimir Vdovjak,
magistar inženjer elektrotehnike

# HOAX

*UDK: 343.533:004*
*Pregledni znanstveni rad*
*Primljeno: 20.05.2012.*

Moderno informacijsko društvo prate njegovi brojni suputnici od kojih je jedan od najopasnijih računalni kriminalitet. Pod pojmom «računalni kriminalitet» smatra se ukupnost počinjenih kaznenih djela kojima se neovlašteno utječe na uporabu, cjelovitost i dostupnost tehničke, programske i podatkovne osnovice računalnog sustava ili na tajnost digitalnih podataka bez obzira kolika šteta nastane usljed njih. Zloporabe ovakve vrste danas postaju sve učestalije, a posljedice sve opasnije. S obzirom da je moderna računalna tehnologija svakim danom sve razvijenija i dostupnija, slobodno se može reći da se gotovo istom brzinom razvijaju i različite vrste njezinih zloporaba koje se u današnjem suvremenom svijetu nikako ne smiju zanemariti. Jedna od najčešćih metoda manipuliranja računalima jest hoax, e-mail poruka koja na prvi pogled izgleda bezazleno, ali eventualne posljedice se ne trebaju smatrati zanemarivima. U ovom radu razlaže se što je hoax, koje su njegove posljedice i pravna zaštita prema odredbama Kaznenog zakona Republike Hrvatske.

**Ključne riječi:** *Kazneni zakon, Konvencija o kibernetičkom kriminalu, elektronička pošta, računalni kriminalitet*

## 1. UVOD

Kada se govori o računalnom kriminalitetu, prvo na što se pomisli su metode manipuliranja računalima poput neovlaštenog pristupa računalnom sustavu, zaraze sustava virusima, manipuliranje podacima, trojanski konji i mnoge druge metode. Međutim, među pojavne oblike računalnog kriminaliteta ubraja se i nešto blaži oblik računalnog krimininaliteta koji se naziva hoax koji je i glavna tema ovog rada.

U nastavku rada pobliže ćemo govoriti o pojmu hoax, njegovom sadržaju te kako ga prepoznati. Opisat ćemo postojeće oblike hoaxa te navesti primjere, a reći ćemo nešto i o motivima za pokretanje hoaxa te postoji li realna opasnost od njegovog širenja.

## 2. ŠTO JE HOAX?

Hoax je poruka elektroničke pošte kojoj je cilj da ljude uvjeri kako je nešto istinito iako je to, zapravo, lažno [1]. Temelji se na neprovjerenim činjenicama i dokazima koji, na pri pogled, mogu izgledati stvarno.

Drugim riječima, hoax je poruka elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Želja osobe koja je poslala hoax je njegovo prosljeđivanje na što veći broj adresa. Pri tome ga primatelj prosljeđuje internetom uvjeren da time pomaže drugima.

Hoaxi ne mogu uzrokovati oštećenja računalnih programa i operacijskih sustava, ali zabilježeni su brojni slučajevi gdje su hoaxi svojim sadržajem i vještom psihologijom naveli korisnike da sami oštete svoje programe i sustave. Drugi oblik štete koji hoaxi nanose korisnicima je zavaravanje korisnika te narušavanje njihovog ugleda kao i ugleda određenih organizacija, tvrtki i poznatih osoba. Treći oblik štete je nepotrebno zagušivanje propusnosti mreže, a četvrti potencijalni negativni financijski učinak.

### 2.1. Različiti sadržaji hoaxa

Kako bi naveli primatelja da proslijedi primljenu poruku na što veći broj adresa, tvorci hoaxa služe se različitim tehnikama, zavisno od sadržaja poruke[2]. Ako hoax upozorava na neki opasan virus, tada se tvorci hoaxa obično služe stručnom terminologijom, dok kredibilitet pokušavaju postići pozivanjem na poznate tvrtke. Nasuprot tome, sadržaj hoaxa koji predstavlja pismo majke bolesnog djeteta kojoj će neka organizacija donirati određenu količinu novaca za operaciju, proporcionalnu broju primatelja poruke, koristi se drugom psihologijom uvjeravanja. Tvorci takvog hoaxa ciljaju na osjećajnost primatelja koji ne želi odmoći tom djetetu, te stoga prosljeđuje poruku poznanicima.

### 2.2. Hoax i psihologija čovjeka

Većina tvoraca hoaxa cilja na čovjekovu prirodnu potrebu da pomogne drugim ljudima. Pomoć može biti usmjerena nekome koga ne poznajemo ili onima koje poznajemo. Hoaxi koji upozoravaju na "opasne" viruse koji uništavaju računalne programe ili "strašne stvari" koje vrebaju iza ugla, djeluju na primatelja tako da on želi upozoriti svoje prijatelje i tako im pomoći. Hoaxi koji traže pomoć od primatelja također pobuđuju kod primatelja potrebu za pomaganjem pa primatelj bez puno razmišljanja prosljeđuje poruku dalje. Tvorci hoaxa mogu ciljati na čovjekovu potrebu za zaradom i srećom koja će ih sustići ukoliko proslijede poruku. U tom slučaju može se govoriti o čovjekovoj potrebi da pomogne samom sebi.

[1] www.infosecwriters.com / text_resources / pdf / Hoax_DCobaugh.pdf

[2] www.carnet.hr

### 2.3. Hoax u Republici Hrvatskoj

Za razliku od ostatka svijeta gdje vrlo visok postotak stanovništva ima pristup internetu, u Hrvatskoj poruke hoaxa posljednjih godina nisu imale velik udio u prometu elektroničke pošte. Većina uočenih hoaxa bili su na engleskom jeziku, koji je i neslužbeni univerzalni jezik komunikacije na internetu.

S obzirom na činjenicu da u Hrvatskoj sve veći broj stanovništva ima pristup internetu te da se hoax poruke i u Hrvatskoj popularizira, CARNet CERT (Computer Emergency Response Team) je uveo uslugu razotkrivanja hoaxa.

## 3. NAJČEŠĆI OBLICI HOAXA

### 3.1. Hoaxi kao upozorenja o štetnim programima

Hoaxi kao upozorenja o štetnim programima obično sadrže lažna upozorenja o novim, "jako opasnim" virusima i crvima, trojanskim konjima ili drugim oblicima malicioznog programskog koda [3]. Korisnici koji prime takva upozorenja prosljeđuju ih svojim poznanicima s dobronamjernim ciljem da ih upozore.

Činjenica da pravi zlonamjerni programski kodovi mogu korisnicima uzrokovati ozbiljne probleme pruža tvorcima hoaxa velike mogućnost prilikom pisanja lažnih upozorenja. Upozorenje kako bi potencijalni virus ili crv mogao uzrokovati brisanje svih podataka, oštećenje diska, BIOS-a i slično kod neiskusnih korisnika uglavnom ostvaruje cilj, tj. utječe na njih da upozore svoje poznanike.

Organizacije koje tvorci ovih upozorenja uglavnom navode kako bi kod primatelja stekli kredibilitet i vjerodostojnost napisanog su: IBM, Microsoft, AOL, Norton, Symantec, McAfee, te mnoge druge organizacije kojima je osnovni posao računalna sigurnost. Osim stručnih organizacija, tvorci hoaxa često navode i neke pouzdane informacijske medije, od kojih je najčešći CNN.

### 3.2. Hoaxi koji navode korisnika da sam ošteti svoj računalni sustav

Hoaxi ovog tipa mogu svojim sadržajem i vještom psihologijom navesti korisnike da sami oštete svoje programe i sustave. Ukoliko poruka sadrži naputak kako primatelj vjerojatno već posjeduje novootkriveni virus te da isti treba ukloniti sa svog sustava, primatelj može podleći takvom lažnom upozorenju. Prevareni primatelj je nakon toga upućen locirati datoteku za koju vjeruje da je neki oblik malicioznog koda i obriše je sa sustava. Ako primatelj to napravi, najvjerojatnije više neće moći koristiti određeni program ili cijeli sustav na ispravan način. Primjer takvih hoaxa su Sulfnbk.exe i Jdbgmgr.exe za koje se navodi da su opasni virusi koji će se aktivirati nakon određenog vremena, dok su oni zapravo bitni dijelovi brojnih aplikacija operacijskih sustava Windows.

[3] www.carnet.hr

### 3.3. Istinita upozorenja koja su prerasla u hoaxe

Za razliku od većine hoaxa koji su u potpunosti lažni, neki hoaxi nisu u potpunosti neistiniti. Primjer takvog hoaxa je i PKZ300 koji upozorava na trojanskog konja pod istim imenom. Taj isti trojanski konj postoji, ali evidentirana šteta koju je nanio je izrazito mala u odnosu na cirkuliranje upozorenja o tom istom hoaxu. Nasuprot takvim hoaxima, postoje i hoaxi koji upozoravaju na programe koji su ispravni i mogu se skinuti s Interneta. Ti programi mogu biti obični bezazleni grafički programi, PowerPointove prezentacije i sl., dok se u hoaxima navodi da su različiti oblici malicioznih programskih kodova. Primjer takvih hoaxa su i Ghost.exe, Make Money Fast i brojni drugi.

#### *3.3.1. Neka lažna upozorenja na maliciozne kodove:*

- PKZ300 - pravi trojanski konj koji nije opasan u mjeri u kojoj je to navedeno u hoaxu
- How to Give a Cat a Colonic - naziv e-mail poruke za koju se neopravdano tvrdi da uzrokuje brisanje datoteka
- Irina - e-mail za koji se neopravdano tvrdi da sadrži kôd koji prepisuje disk
- Good Times - nepostojeći virus za koji se navodi da uzrokuje brisanje diska
- Deeyenda - nepostojeći virus za koji se tvrdi da uzrokuje prepisivanje diska
- Ghost.exe - program za koji se neopravdano navodi da je trojanski konj
- Make Money Fast - program za koji se neopravdano navodi da uzrokuje brisanje particija
- Join the Crew - naziv e-maila za koji se neopravdano tvrdi da uzrokuje brisanje diska
- Death Ray - nepostojeći virus za koji se navodi da uzrokuje oštećenja čak i na sklopovlju računala
- A.I.D.S. - nepostojeći virus za koji se navodi da uzrokuje brisanje diska
- Bud Frogs Screen Saver - screen saver za koji se lažno navodi da je trojanski konj
- Bug's Life Screen Saver - screen saver za koji se lažno navodi da je trojanski konj
- WIN A HOLIDAY - naziv e-maila za koji se neopravdano tvrdi da uzrokuje brisanje datoteka
- Jdbgmgr.exe - dio operacijskog sustava lažno opisan kao virus
- Sulfnbk.exe - dio operacijskog sustava lažno opisan kao virus
- Life Is Beautiful Hoax - PowerPointova prezentacija za koju se lažno tvrdi da će nakon otvaranja izbrisati sve podatke s diska i pošiljatelju poslati autentikacijske podatke

### *3.3.2. Primjer lažnog upozorenja o štetnom programu*

Sljedeći primjer hoaxa pod nazivom Flashmaster G upozorava primatelja da proslijedi primljenu poruku na što veći broj adresa. Kao razlog tomu navodi se da Internetom kola e-mail s datotekom pod nazivom Flashmaster G koja je zapravo virus El Poco. Prema sadržaju hoaxa, spomenuti virus uzrokuje brisanje tvrdog diska i rušenje mreže, što danas niti jedan poznati virus ne može učiniti.

### *3.3.3. Primjer hoaxa koji upućuje korisnika na oštećenje vlastitog računalnog sustava*

"JDBGMGR.EXE" je trenutačno najpopularniji i najuspješniji hoax koji korisnike navodi na oštećenje vlastitih računalnih sustava. Korisnika se navodi na uništavanje datoteke jdbgmgr.exe. Iako spomenuta datoteka nije ključna za rad Windows sustava, brojne Java aplikacije ipak ovise o njoj. Unutar ovog hoaxa posebna je važnost posvećena opisivanju akcija koje korisnik treba učiniti. CARNet CERT u svojoj hoax bazi posjeduje brojne primjerke slične dolje navedenom. Unatoč tome, svakodnevno se otkrivaju novi uzorci s istom temom, a koje je potrebno nanovo unijeti u bazu.

### *3.3.4. Lanci sreće i zarade*

Lanci sreće i zarade su hoaxi u kojima se primatelju za prosljeđivanje primljene poruke na određen broj adresa obećava novac, besplatni mobiteli, putnički aranžmani, pokloni ili uspjeh u životu. Lanci sreće mogu imati i prijeteći karakter. U tim slučajevima primatelja se upozorava kako će ga pogoditi nesretan i neugodan događaj ukoliko primljenu poruku ne proslijedi na što veći broj adresa.

#### *3.3.4.1. Lanci sreće*

Lance sreće lakše je prepoznati nego primjerice hoaxe koji upozoravaju na maliciozne kodove. Tome pridonosi i činjenica da su postojali i prije nastanka Interneta, samo što su se tada prosljeđivali klasičnom poštom. Takve e-mail poruke čak i najneiskusniji korisnici Interneta mogu razotkriti kao lažne upravo zahvaljujući njihovom sadržaju. Usprkos tome, lanci sreće prelaskom u doba Interneta dobili su na intenzitetu zbog prednosti u odnosu na klasični način. Prednosti koje e-mail poruke imaju u odnosu na klasičnu poštu su jednostavnost prosljeđivanja i besplatno slanje. Činjenica da su se lanci sreće održali u obliku klasične pošte, gdje je to kompliciranо i skupo, govori koliki je promet moguć i u obliku e-mail poruka, koje su besplatne i jednostavne za rukovanje.

#### *3.3.4.2. Lanci zarade*

Lance zarade teže je prepoznati u odnosu na lance sreće. Dok je kod lanaca sreće bitan faktor praznovjernost korisnika, lanci zarade oslanjaju se na ljudsku osobinu povezanu sa zaradom, tj. pohlepu. Na neodlučne primatelje hoaxa često utječe činjenica da prosljeđivanjem primljene sumnjive poruke ništa ne mogu izgubiti, a ipak nešto mogu dobiti. Zbog toga se brojni korisnici odlučuju na

prosljeđivanje. Tvorci hoaxa se pri tome koriste raznim lažnim obećanjima kako bi zaveli primatelja i naveli ga da proslijedi poruku osobama u adresaru.

Tvorci hoaxe bazirane na zaradi zasnivaju na lažnim darivanjima novca i poklona. Izmišljeni pokloni uglavnom su manje vrijedni, kao što su besplatne majice, kape i sl. Pri tome se kao autor e-mail poruke najčešće navodi neka organizacija koja proizvodi navedene proizvode. Kao razlog izdavanja e-mail poruke najčešće se navode marketinški razlozi.

*3.3.4.2.1. Primjeri lanaca zarade i njihovih poklona:*

- Bill Gates - Bill Gates daruje određenu količinu novaca za svaki prosljeđeni e-mail.
- Disney Giveaway - Disney daruje određenu količinu novaca za svaki prosljeđeni e-mail kao i besplatni put u Disneyworld.
- Netscape-AOL Giveaway - Netscape i AOL daruju određenu količinu novaca za svaki prosljeđeni e-mail.
- Ericsson Phone Giveaway i Nokia Phone Giveaway - Ericsson, tj. Nokia daruju besplatne mobitele za određeni broj prosljeđenih e-mailova.
- Honda Giveaway - Honda daruje novi automobil za određeni broj prosljeđenih e-mailova.

Neki hoaxi otvoreno navode da je njihov cilj prosljeđivanje e-maila što većem broju korisnika i to se pritom objašnjava raznim objašnjenjima kao što su sljedeća:

- World Record Hoax - kao razlog navodi se cilj ulaska u Guinnessovu knjigu rekorda.
- Helping Kids With School Project Chain - kao razlog navodi se jedan školski projekt grupe školaraca koji izučavaju put odaslane e-mail poruke. Projekt je postojao, ali je odavno završio, dok ljudi i dalje prosljeđuju ovaj e-mail.

*3.3.4.2.2. Primjer lanca zarade*

Sljedeći primjer pod nazivom "Bill Gates Hoax" veoma je raširen primjer lanca zarade. Njegov navodni kreator je Bill Gates, većinski vlasnik Microsofta. U ovom se hoaxu od primatelja traži prosljeđivanje primljene e-mail poruke na što veći broj adresa - ukoliko taj broj posredno prijeđe 1000, Bill Gates će donirati 1000 USD i instalacijski CD s Windowsima 98. Koliko je ovaj hoax star pokazuje i činjenica da se daruju Windowsi 98. U ovom primjeru je također moguće uočiti u hoaxima često navođenu neistinitu činjenicu kako je moguće pratiti promet e-mail poruke.

## 4. LAŽNI ZAHTJEVI ZA POMOĆ

Lažni zahtjevi za pomoć su e-mail poruke kojima se kod primatelja izaziva suosjećanje prema nemoćnim osobama, obično djeci, i traži pomoć prosljeđivanjem primljene poruke. Primatelji ovakvih hoaxa rijetko odbijaju pomoći primjerice nekom bolesnom djetetu te je zbog toga ova vrsta hoaxa veoma raširena.

### 4.1. Uobičajeni razlozi lažnih zahtjeva

Tvorci ovakvih hoaxa u svojim porukama navode različite razloge za prosljeđivanje primljene poruke. Velik broj hoaxa zasniva se na priči o bolesnom djetetu kojemu će određena organizacija darovati sumu novaca proporcionalnu broju proslijeđenih e-mail poruka. Važna činjenica koja razotkriva ove hoaxe je što niti jedna organizacija ne može pratiti put e-mail poruke.

Osim uobičajene teme o određenim organizacijama koje daruju novac bolesnoj djeci, mogući su i drugi razlozi za prosljeđivanje povezani s bolesnom djecom. Neki hoaxi zasnivaju se na laži da je djetetova zadnja želja bila da njegova e-mail poruka nastavi putovati svijetom.

Uz spomenute, česti su i hoaxi u kojima navodni roditelji traže od primatelja da proslijede poruku u kojoj je slika izgubljenog djeteta. Zanimljivo je da su neke od današnjih e-mail poruka povezane s izgubljenom djecom nekada i bile istinite. Roditelji su zaista u Americi slali poruke u kojima mole pomoć pri potrazi za izgubljenim djetetom, ali danas je kod tih e-mail poruka problem što se jednom poslan e-mail više ne može lako zaustaviti. Zbog toga korisnici danas prosljeđuju razne e-mail poruke koje više nisu aktualne pa stoga nepotrebno troše tuđe, a i svoje vrijeme, kao i računalne resurse.

### 4.2. Najčešći lažni zahtjevi za pomoć su:

- Jessica Mydek - hoax u kojem se navodi da će za svaki proslijeđeni e-mail American Cancer Society donirati tri centa za operaciju smrtno bolesne Jessice Mydek.
- Anthony Parkin - hoax koji je navodno pokrenuo umirući Anthony Parkin u želji da nikad ne umre, barem na Internetu.
- Kelsey Brooke Jones Warning - lažno upozorenje o izgubljenoj djevojčici koja je zaista bila izgubljena, ali samo nekoliko sati. Kasnije je pronađena kako se igra kod susjede. Ovaj e-mail se, nažalost, i dalje pronalazi na Internetu, četiri godine nakon što je nastao.
- Penny Brown Hoax - lažni zahtjev za pomoć u potrazi za izmišljenom djevojčicom Penny Brown.

### 4.3. Primjer tipičnog lažnog zahtjeva za pomoć

Sljedeći primjer pod nazivom "Rachel Arlington" je jedan od najčešćih lažnih zahtjeva za pomoć te se može pronaći na većini web-stranica koje se bave hoaxima. Ovaj e-mail navodno je napisao George Arlington, otac djevojčice Rachel. U ovoj inačici naznačeno je da djevojčica ima deset mjeseci, a u istom tom upozorenju koje datira iz 2000. navedeno je da ta Rachel ima deset godina. Od primatelja se traži prosljeđivanje e-mail poruke što većem broju poznanika jer na taj način mogu pomoći smrtno bolesnoj Rachel. U slučaju da se poruka proslijedi na tri različite adrese, navedeno je da će AOL i ZDNet donirati 32 centa za operaciju. Tipično za hoaxe, nije navedeno kako će te dvije organizacije pratiti put e-mail poruke.

## 5. ZASTRAŠUJUĆI I PRIJETEĆI HOAXI

Zastrašujući i prijeteći hoaxi su e-mail poruke koje upozoravaju na "opasne" stvari koje se ljudima događaju te pokušavaju zastrašiti primatelje s ciljem da proslijedi upozorenje svojim prijateljima i poznanicima [4].

Moguće je da hoax sadrži i direktnu prijetnju primatelju kojem bi se trebalo nešto "strašno" dogoditi ukoliko ne proslijedi primljeni e-mail. Najčešće se primatelj upozorava kako mora proslijediti primljeni e-mail na određeni broj adresa jer je zajedno s porukom stigao i virus koji može biti otklonjen jedino prosljeđivanjem određenog broja poruka.

### 5. 1. Hoaxi povezani za terorističkim napadom 11. rujna 2001.

Nakon terorističkog napada 11. rujna 2001. na Internetu se pojavila velika količina hoaxa koji upozoravaju na brojne sumnjive aktivnosti određenih građana, uglavnom Arapa. U takvim upozorenjima navode se različiti sumnjivi oblici ponašanja osoba arapskog porijekla, kao što su sljedeći:

- Sumnjivi Arap upozorio jednu osobu da ne pije Coca-Colu nakon određenog datuma.
- Arapi osumnjičeni za krađu kamiona diljem SAD-a.
- Arapi kupuju velike količine slatkiša koji se u SAD-u tradicionalno dijele djeci na Dan vještica.

Iako u Hrvatskoj ovakvi hoaxi ne mogu uzrokovati pomutnju i uznemiriti građane, CARNet CERT je ipak odlučio u svoje baze uzoraka uključiti i hoaxe s terorističkim sadržajima.

### 5. 2. Stvarna opasnost za primatelja ove vrste hoaxa

Zabilježeni su brojni slučajevi u kojima e-mail sadrži tekst u kojem se primatelja upozorava na razne opasnosti. Iako je moguće da su neke od tih opasnosti istinite,

[4] www.carnet.hr

korisnicima se ne preporučuje da prosljeđuju ikakva upozorenja jer postoje brojne organizacije i mediji koji su za to zaduženi. Ukoliko korisnici ipak nastave prosljeđivati upozorenja koja se kasnije pokažu lažnima, to može samo narušiti njihov ugled i vjerodostojnost kod primatelja.

Primjeri u kojima se korisnika upozorava na neke "opasne" stvari koje su se dogodile drugim osobama:

- Shampoo Causes Cancer - lažno upozorenje kako šampon za kosu uzrokuje rak. Kao razlog tomu navodi se izmišljena činjenica da proizvođači radi uštede stavljaju u šampone tvari koje se koriste za pranje automobila i tome sl.
- Lethal Rat Urine - lažno upozorenje o brojnim slučajevima osoba koje su umrle jer nisu oprale konzerve kupljene u trgovinama. Pri tome je navedeno da su konzerve bile pokrivene štakorskim urinom.
- Kidney Harvest - lažno upozorenje o osobi koju su nepoznate osobe opile te se ta osoba drugo jutro probudila bez bubrega.
- Flesh Eating Bananas - lažno upozorenje koje indicira da su neke banane zaražene bakterijom koja proždire meso. Pri tome se od primatelja traži da izbjegava banane (u jednom primjeru iz Kostarike) i da proslijedi e-mail.
- Bad Guy Selling Perfume - lažno upozorenje na osobe koje ispred trgovina prodaju parfeme, koji su zapravo eter. Te izmišljene osobe navode ostale kupce (uglavnom žene) da pomirišu parfem te ih potom onesviještene opljačkaju.

### 5. 3. Primjer tipičnog prijetećeg hoaxa

Sljedeći primjer pod nazivom "Slavemaster" tipični je zastrašujući hoax. Kao tema (subject) e-mail poruke navedeno je "Policijsko upozorenje", što kod brojnih primatelja uzrokuje povećanu pozornost. U njemu se od primatelja traži prosljeđivanje primljene e-mail poruke što većem broju poznanika jer im na taj način može pomoći. U e-mail poruci se upozorava na određenu osobu koja na Internetu koristi nadimak Slavemaster i za koju policija upozorava da je ubila 56 ženskih osoba. Osim što se od primatelja traži prosljeđivanje primljene poruke, primatelja se ujedno upozorava da izbjegava ikakav kontakt s osobom koja koristi spomenuti nadimak. U poruci je zabilježena i tipična pojava stjecanja kredibiliteta pozivanjem na ozbiljne organizacije (u primjeru Yahoo, AOL i Excite).

## 6. LAŽNE PETICIJE

Lažne peticije su e-mail poruke koje imaju različite sadržaje, a u kojima se poziva na sakupljanje "potpisa" za neku izmišljenu ili neizmišljenu važnu stvar te prosljeđivanje poruke kako bi i drugi korisnici mogli dati podršku [5]. Proučavanjem je utvrđeno da se od primatelja uglavnom traži ime i prezime, a ponekad i e-mail

[5] www.carnet.hr

adresa.

Peticije mogu imati izmišljenu ili istinitu temu. Činjenica da je tema na koju se peticija odnosi istinita ne znači da je i sama peticija istinita. Često autori izmišljaju lažne peticije s istinitim temama kako bi uzrokovali pomutnju i potakli beskorisno trošenje tuđih vremenskih i računalnih resursa. Pri tome najčešće krivotvore autora.

### 6. 1. Osnovne postavke neispravne peticije

U slučaju primitka e-mail poruke koja poziva na dodavanje svog "potpisa" na listu i prosljeđivanje iste, potrebno je znati osnovne postavke svake peticije. Njihovom provjerom primatelj lažne peticije može istu i identificirati.

### 6. 2. Osnovne postavke nelegitimne peticije:

- *Nejasan cilj* - peticija ne smije biti neodređena. Peticija mora sadržavati osnovnu listu ključnih točki na koje se peticija odnosi. Ukoliko je lista neodređena ili nije jasno kome će ti rezultati biti proslijeđeni, peticija je vrlo vjerojatno izmišljena. Ako je u peticiji naznačeno da rezultate peticije treba poslati direktno određenoj ustanovi ili osobi na koju se pokušava utjecati, peticija je vjerojatno lažna. Razlog tomu je nevjerojatnost da ta ustanova ili osoba bilježi i sortira dobivene informacije pa je očit cilj stvarnog autora trošenje tuđih vremenskih i računalnih resursa.
- *Lažna privatnost* - brojne peticije napominju da je riječ o anonimnim peticijama. Ako je peticija anonimna, onda se ona može lako i izmisliti, tj. imena se mogu lako dodati. Ukoliko se u sadržaju lažne peticije od primatelja traži upisivanje imena, prezimena i e-mail adrese, peticija ne može biti anonimna jer ostali primatelji e-mail poruke mogu vidjeti tko se sve potpisao.
- *Anonimnost autora* - peticija se može u potpunosti smatrati nepouzdanom ako autor nije naveden. Ako je to slučaj, onda je jasno da niti jedna organizacija neće proučavati rezultate dobivene prosljeđivanjem peticije pa peticija gubi smisao. Većina lažnih peticija sadrži ime autora ili određenu organizaciju koji zaista postoje, ali nisu povezani s tom peticijom.
- *Neodređeno vrijeme postojanja peticije* - ukoliko peticija nema rok do kojeg je važeća, ona je zasigurno lažna. Niti jedna ozbiljna organizacija ne bi stavila peticiju bez naznake njenog "roka trajanja". Svaka peticija mora imati točno određen rok provođenja.

### 6. 3. E-mail-peticije nisu legitimno sredstvo skupljanja "potpisa"

Koncept prikupljanja potpisa putem Interneta nepouzdan je i neuvjerljiv. Bilo tko se može dosjetiti da dopiše određen broj imena te na taj način krivotvori peticiju. Zbog toga se peticija dobivena razašiljanjem e-mail poruka smatra nepouzdanom i nevažećom. Većina organizacija toga je svjesna te zbog toga ne koriste e-mail

poruke za skupljanje potpisa.

### 6. 4. Primjeri u kojima se od primatelja traži "potpisivanje" peticije i njeno prosljeđivanje što većem broju poznanika:

- *Petition to CNN for the Children* - peticija u spomen poginulih u WTC-u 11.09.2001. koja traži od primatelja 'potpis' i prosljeđivanje primljene e-mail poruke. Kao rezultat navedeno je kako će CNN objaviti rezultate peticije.
- *Petition to Stop Animal Abuse in Korea* - peticija pomoći zlostavljanim životinjama u Koreji koja se odnosi na sprečavanje narodnih običaja u Koreji, a koji uključuju pse i mačke kao hranu. Autor peticije je anoniman, a rok nije određen.
- *The Racism Petition* - antirasistička peticija sa anonimnim autorom, bez jasnog cilja i naznačenog roka.
- *AOL Price petition* - peticija koju je navodno AOL pokrenuo, a navodi se kako u slučaju velikog broja 'potpisa' AOL sniziti svoje cijene. Peticija u potpunosti ne zadovoljava prethodno određene osnovne postavke ispravne peticije.
- *Amazon rain forest petition* - peticija koja se odnosi na prijedlog iz 2000. godine koji je brazilski kongres trebao razmatrati. Tim prijedlogom predviđeno je krčenje šuma i uzgoj drugih agrokultura. Prijedlog je odbačen još 2000. godine, dok peticija i dalje kruži Internetom.

### 6. 5. Primjer lažne peticije

Sljedeći primjer pod nazivom "Petition to Help Zimbabwe" reprezentativan je primjerak tipične lažne peticije. Peticija se odnosi na potpomaganje demokracije u Republici Zimbabve. Pri tome je autor napravio brojne propuste koji ovaj uzorak nepogrešivo označuju kao lažni hoax. U tekstu nije navedeno tko je autor peticije, a kao adresa slanja rezultata peticije navedena je Bijela kuća. Ti detalji su i najnelogičniji jer peticiju nije pokrenula Bijela kuća, pa nitko nije zadužen za obradu peticijskih e-mail-poruka. Tekst poruke ne sadrži primjere na temelju kojih bi se utvrdilo da je Robert Mugabe (predsjednik Zimbabvea) zaista diktatorski manijak. U peticiji nije navedeno kada je pokrenuta, tko ju je pokrenuo i do kada traje, što je u potpunosti deklasira kao legitimnu peticiju.

## 7. KOMPROMITIRAJUĆI HOAXI

Kompromitirajući hoaxi su e-mail poruke koje narušavaju ugled određenih organizacija, tvrtki ili osoba. Takve poruke sadrže lažne ili iskrivljene navode i glavni im je cilj narušavanje nečijeg ugleda. Ti lažni navodi (tračevi) navode prevarene primatelje na prosljeđivanje poruke poznanicima. Pri tome se najčešće od primatelja traži bojkotiranje određene organizacije, tvrtke ili osobe.

### 7. 1. Razlozi i posljedice kompromitiranja

Razlozi za kompromitiranje određene osobe ili organizacije mogu biti različiti. Određene osobe iz osobnih razloga, čiste zlobe ili dosade mogu pokrenuti lažne kompromitirajuće e-mail poruke. Pritom se tvorac hoaxa može služiti brojnim psihološkim trikovima da uvjeri primatelja u istinitost poruke. Primjer je pozivanje na priznate organizacije koje su prethodno navodno objavile navedenu obavijest.

### 7. 2. Razotkrivanje kompromitirajućih hoaxa

Zbog opasnosti da je primljena e-mail poruka zapravo kompromitirajući hoax, ne preporuča se prosljeđivanje poruka sličnog sadržaja. Ukoliko se takav hoax nastavi prosljeđivati Internetom, oklevetana organizacija ili osoba mogu pretrpjeti veliku štetu u obliku narušavanju ugleda, a moguća je i financijska šteta. Zbog toga je za sumnjive e-mail poruke najbolje rješenje potražiti mišljenje od ovlaštenih organizacija, poput CARNet CERT-a.

### 7. 3. Česti kompromitirajući hoaxi uočeni na Internetu

- Harry Potter Hoax - hoax u kojem se za J. K. Rowling, autoricu knjige "Harry Potter", tvrdi da je sotonistica. U toj poruci se primatelja upozorava da knjige "Harry Potter" utječu negativno na dječji kršćanski duh.
- Boycott Tommy Hilfiger Hoax - hoax u kojem se navodi da je proizvođač odjeće Tommy Hilfiger, u emisiji Oprah Show - u kojoj nikad nije gostovao, dao rasističku izjavu. On je navodno izjavio kako ne voli da crnci, židovi, latinoamerikanci i azijci kupuju njegovu odjeću. U poruci se poziva na bojkot njegove odjeće.
- McDonalds Beef Warning - hoax koji se zasniva na američkom domoljublju. U njemu se poziva na bojkot restorana McDonalds jer neregularno uvoze meso iz južnoameričkih država. McDonalds je opovrgnuo navedenu tvrdnju.
- Bill Clinton Hoax - hoax u kojem se navodi da je bivši američki predsjednik Bill Clinton, za svog mandata, amnestirao glavnu osobu odgovornu za napade na New York 11. rujna 2001.

### 7. 4. Primjer kompromitirajućeg hoaxa

Kompromitirajući hoax pod nazivom Procter & Gamble Hoax jedan je od najčešće uočenih hoaxa na Internetu. Ta lažna e-mail poruka datira još iz 1999. godine. U njoj se upozorava da je predsjednik tvrtke Procter & Gamble pripadnik sotonističke crkve i da velik dio svojih prihoda prosljeđuje toj tobožnjoj ustanovi. Zbog toga se primatelja ove poruke moli da bojkotira sve proizvode organizacije Procter & Gamble.

## 8. BEZAZLENI HOAXI

Bezazleni hoaxi su e-mail poruke za koje primatelji uglavnom odmah shvate da su lažne, ali ih nastavljaju prosljeđivati zbog njihovog šaljivog sadržaja. Većina korisnika voli primati ovakve e-mail poruke, pa zbog toga CARNet CERT uglavnom nije niti uvrštavao ove uzorke u svoju bazu. Ipak, zbog manjeg broja korisnika koji ne shvate odmah da je zaista riječ o hoaxima, najpopularniji hoaxi ove vrste uvršteni su u CERT-ovu bazu.

### 8. 1. Neki bezazleni hoaxi uočeni na Internetu:

- *Taliban virus* - siromašni talibani ne umiju isprogramirati virus pa primatelja e-mail poruke mole da sam razbije svoje računalo.
- *Internet Cleanup Day* - upozorenje da se određenog dana ne posjećuje Internet jer se tog dana čisti Internet.
- *Launch Nuclear Strike Now Joke* - upozorenje da primatelj nikako ne smije otvoriti e-mail poruku pod nazivom Launch Nuclear Strike Now jer će time uzrokovati nuklearni napad SAD-a na Rusiju.
- *Picture Through Your Monitor Joke* - e-mail poruka koja primatelja poziva da posjeti web-stranicu na kojoj će primiti svoju sliku snimljenu "posebnom metodom". Stranica je sljedeća: http://www.geocities.com/Heartland/Acres/3072/camera1.html.

## 9. KAKO PREPOZNATI HOAX?

U većini slučajeva iskusni korisnici mogu lako razaznati da li je primljena poruka hoax ili ne [6]. Jedan od glavnih pokazatelja je rečenica: "Pošaljite ovu poruku na što veći broj adresa!" Međutim, pošto se tvorci hoaxa služe stručnom terminologijom, a kredibilitet pokušavaju postići pozivanjem na poznate tvrtke, korisnici ne mogu uvijek uvidjeti da je poruka lažna.

### 9. 1. Opće odrednice pri razotkrivanju hoaxa

- Sadrže izravan ili posredan zahtjev da se poruka proslijedi, kao što je: "Pošaljite ovu poruku na što veći broj adresa!"
- često se pozivaju na različite priznate organizacije, što zavisi o sadržaju hoaxa,
- naglašavaju kako primatelj prosljeđivanjem poruke može pomoći sebi ili drugima.

Najuspješniji način razotkrivanja hoaxa je njihovo klasificiranje u jednu od navedenih skupina koje slijede.

[6] www.carnet.hr

### *9.1.1. Hoaxi kao upozorenja o štetnim programima*

- Upozoravaju na određenu vrstu malicioznog koda koji uzrokuje brisanje svih podataka, nepopravljivo oštećenje diska ili BIOS-a, oštećenje sklopovlja računala i sl. Na sreću, virusi koji uzrokuju navedeno ne postoje.
- Pozivaju se na stručne informatičke i medijske organizacije kao što su: -IBM, Microsoft, AOL, McAfee, Norton, Symantec, CNN
- Upozoravaju da je potrebno obrisati određenu datoteku s računala jer je najvjerojatnije maliciozni kod. Najčešće je ta opasna datoteka legitimna datoteka ključna za rad operacijskog sustava.

### *9.1.2. Lanci sreće i zarade*

- Sadrže poruku da se prosljeđivanjem poruke može zaraditi velika svota novaca ili dobiti razni pokloni od različitih organizacija kao što su:

  -novac i informatička oprema koju daruju IBM, Microsoft (Bill Gates), AOL,

  -auti koji daruje Honda

  -odjeća koju daruju GAP, Nike, ...

  -mobiteli koje daruju Nokia, Ericsson, Simmens, ...
- Sadrže poruku da će primatelja pratiti velika sreća koja je najčešće proporcionalna broju proslijeđenih poruka. Isto tako, u slučaju neprosljeđivanja, navodi se da će primatelja pogditi nesreća.

### *9.1.3. Lažni zahtjevi za pomoć*

- Upozoravaju da se prosljeđivanjem poruke može pomoći određenoj bolesnoj osobi ili osobama, najčešće djeci.
- Sadrže poruku da određene velike informatičke organizacije (Microsoft, AOL…) mogu pratiti primljenu e-mail poruku i da će za svaku proslijeđenu poruku biti donirana određena suma novaca. Važno je napomenuti da niti jedna organizacija ne može pratiti put određene e-mail poruke.
- Često napominju da je djetetova zadnja želja bila da njegova e-mail poruka nikad ne prestane putovati Internetom.
- U slučaju spominjanja djece (izgubljene ili bolesne) često je u poruku umetnuta i slika.

### *9.1.4. Zastrašujući i prijeteći hoaxi*

- Upozoravaju na neke izrazito "opasne stvari" ili događaje te naglašavaju kako primatelj prosljeđivanjem primljene poruke može pomoći svojim poznanicima.
- Često navode korisnika da proslijedi određen broj e-mail poruka jer je zajedno s e-mail porukom stigao i virus koji može biti otklonjen jedino na taj način.
- U SAD-u su česta upozorenja na Arape i njihove sumnjive djelatnosti.

- Često navode kako su to isto upozorenje objavile i određene priznate medijske organizacije, od kojih se najčešće spominje CNN.

#### *9.1.5. Lažne peticije*

- Nejasan cilj - peticija je neodređena. Kao adresa slanja rezultata peticije ne navodi se autor peticije, već neka organizacija na koju se pokušava utjecati.
- Lažna privatnost – brojne peticije napominju da je riječ o anonimnim peticijama, što je nemoguće ostvariti e-mailom. Ukoliko je peticija anonimna, onda se ona može lako i izmisliti, tj. imena se mogu lako dodati.
- Anonimnost autora – peticija se može u potpunosti smatrati nepouzdanom ako autor nije naveden. Većina lažnih peticija sadrži ime autora ili određenu organizaciju koji zaista postoje, ali nisu povezani s tom peticijom.
- Neodređeno vrijeme trajanja peticije – ukoliko peticija nema rok do kojeg je važeća, ona je zasigurno lažna. Svaka peticija mora imati točno određen rok u kojem se provodi.
- e-mail-peticije nisu priznat i mjerodavan oblik sakupljanja potpisa pa ih ne treba prosljeđivati.

#### *9.1.6. Kompromitirajući hoaxi*

Ne postoje univerzalni pokazatelji ove vrste hoaxa. U slučaju da sadržaj poruke ocrnjuje određenu organizaciju, tvrtku ili osobu, ne preporuča se prosljeđivanje poruke, već se preporuča kontaktiranje ovlaštene organizacije poput CARNet CERT-a.

#### *9.1.7. Bezazleni hoaxi*

Najlakše uočljiva vrsta hoaxa. Glavni pokazatelj im je duhovit i nevjerojatan sadržaj. Kako većina korisnika Interneta voli primati ovu vrstu e-mail poruka, oni nisu sadržani u većoj količini unutar CARNet CERT-ove baze. U CERT-ovim bazama sadržani su samo bezazleni hoaxi koji su najčešći te hoaxi za koje nije lako utvrditi da je zaista riječ o bezazlenim hoaxima.

## 10. MOTIVI ZA POKRETANJE HOAXA

Tvorci hoaxa često nisu niti svjesni da njihove e-mail poruke, početno poslane u dobroj namjeri, tijekom kruženja Internetom izrastaju u neslomljive i nezaustavljive hoaxe [7]. Razlozi zbog kojih određene osobe svjesno kreiraju i puštaju u optjecaj različite hoaxe mogu biti veoma različiti, a najčešće i neshvatljivi. Neki od mogućih motiva za pokretanje hoaxa navedeni su u nastavku.

[7] www.carnet.hr

### 10.1. Pošiljatelji žele vidjeti kako daleko poruka može stići i koliko dugo može egzistirati

Korisnici često pokreću hoaxe jer ih zanima dokud te iste e-mail poruke mogu stići i koliko dugo mogu opstati na Internetu. Nažalost, te poruke često obiđu svijet i po nekoliko puta, a na Internetu opstanu više godina.

### 10.2. Zavaravanje korisnika

Brojni korisnici Interneta poslali su lažnu e-mail poruku nekim svojim poznanicima bez namjere da ta poruka stigne do šireg kruga korisnika. Ipak, pojedinci su nastavili prosljeđivati te e-mail poruke i tako se krug prevarenih proširio. Osim spomenutog, moguće je da tvorci hoaxa namjerno kreiraju određen lažni sadržaj kako bi zavarali što veći broj primatelja i na taj način ostvarili neke svoje ciljeve (političke ili osobne).

### 10.3. Uništavanje ugleda neke organizacije, tvrtke ili osobe (kompromitirajući hoaxi)

Tvorci u svojim lažnim upozorenjima često navode lažne ili iskrivljene činjenice o određenim organizacijama, tvrtkama ili poznatim osobama i pritom primatelje potiču na njihovo bojkotiranje. Ukoliko primatelji povjeruju sadržaju primljene e-mail poruke, tada se, osim narušavanja ugleda, često uzrokuje i financijska šteta.

## 11. KOJA JE OPASNOST OD ŠIRENJA HOAXA

Širenjem hoaxa se ne može izazvati velika šteta. Ipak, hoaxi često zavaravaju korisnike, narušavaju ugled određenih organizacija ili osoba, pritom bespotrebno opterećujući mrežu, povećavaju troškove korištenja Interneta te zatrpavaju Inbox osoba koje dobivaju hoaxe.

### 11.1. Zavaravanje korisnika

Ukoliko hoax uspije prevariti primatelja i on ga proslijedi svojim poznanicima, primatelj ispada naivan. Iako je primatelj možda proslijedio primljenu poruku s ciljem da upozori svoje poznanike, on ipak u očima svojih sumnjičavijih poznanika ispada naivan.

Najveća šteta koja se može uzrokovati zavaravanjem korisnika je oštećenje korisnikovog računalnog sustava. Ako sadržaj hoaxa uvjeri primatelja da je određena datoteka zapravo virus, korisnik bi je mogao obrisati, ne znajući da je ta datoteka zapravo ključan dio računalnog operacijskog sustava.

### 11.2. Narušavanje ugleda organizacija, tvrtki i osoba – moguća i izravna financijska šteta

Kompromitirajući hoaxi mogu narušiti ugled oklevetanih organizacija, tvrtki ili osoba. U slučaju da sadržaj hoaxa zahtijeva od primatelja bojkot određenih proizvoda, moguće je i nanošenje izravne financijske štete.

### 11.3. Nepotrebno opterećenje mreže i povećanje troškova korištenja Interneta

Osim što može štetiti pojedinim osobama ili organizacijama, prosljeđivanje hoaxa šteti i cijeloj internetskoj zajednici. Takve poruke nepotrebno opterećuju mrežu i na taj način uzrokuju povećanje troškova korištenja Interneta.

## 12. KAZNENO-PRAVNA ZAŠTITA

Ovisno o inkriminaciji, hoax se može pronaći u tri članka Kaznenog zakona. To su:

### 12.1. Povreda tajnosti, cjelovitosti i dostupnosti računalnih podataka, programa i sustava [8]

*Članak 223.*

*»(1) Tko unatoč zaštitnim mjerama neovlašteno pristupi računalnom sustavu,*

*kaznit će se novčanom kaznom ili kaznom zatvora do jedne godine.*

*(2) Tko s ciljem onemogući ili oteža rad ili korištenje računalnih podataka ili programa, računalnog sustava ili računalnu komunikaciju,*

*kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(3) Kaznom iz stavka 2. ovoga članka kaznit će se tko neovlašteno ošteti, izmijeni, izbriše, uništi ili na drugi način učini neuporabljivim ili nedostupnim tuđe računalne podatke ili programe.*

*(4) Kaznom iz stavka 2. ovoga članka kaznit će se tko presretne ili snimi nejavni prijenos računalnih podatka koji mu nisu namijenjeni prema računalnom sustavu, iz njega ili unutar njega, uključujući i elektromagnetske emisije računalnog sustava koji prenosi te podatke, ili tko omogući nepozvanoj osobi da se upozna s takvim podacima.*

*(5) Ako je kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka počinjeno u odnosu na računalni podatak, program ili sustav tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta,*

[8] Kazneni zakon NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08.

*počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.*

*(6) Tko neovlašteno izrađuje, nabavlja, uvozi, raspačava, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka,*

*kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(7) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1., 2., 3. ili 4. ovoga članka oduzet će se.*

*(8) Za pokušaj kaznenog djela iz stavka 1., 2., 3. ili 4. ovoga članka počinitelj će se kazniti.*

Člankom 223., stavak 1, opisano je ponašanje koje se odnosi na nezakoniti pristup[9]. Njime se određuje da Zakon štiti samo onaj sustav koji ima zaštitne mjere. Ako se sustav ostavi potpuno otvorenim i nezaštićenim, odnosno ako računalo bude potpuno dostupno, neće se ostvariti elementi kaznenog djela.

U stavku 2. istog članka opisano je ponašanje koje se odnosi na ometanje sustava. U praksi su česti slučajevi koji se ovim stavkom inkriminiraju. Važan element ovdje jest namjera što znači da se oslobađa odgovornosti onaj tko, na primjer, nepažnjom isključi ključna računala davatelja internet usluga i dovede do prekida komunikacije. Ovdje je važno istaknuti da se upravo ovdje može pronaći jedna od specifičnosti vezanih za računalni kriminal. Napadač može pustiti u distribuciju crva koji će se proširiti na tisuće drugih računala, koja će onda, bez znanja svojih rabitelja, sudjelovati u napadu. To bi značilo da postoji mogućnost uporabe tuđe infrastrukture u počinjenju kaznenog djela bez ikakvog znanja vlasnika ili osoba koje rabe tu infrastrukturu. Oni ne mogu kazneno biti odgovorni za zlouporabu svoje opreme, ali će posredno biti njome pogođeni usporavanjem „zaraženih" računala i opterećivanjem njihovih mrežnih veza.

Stavak 3. opisuje ometanje podataka čime se taj oblik imovine štiti slično kao što se štite materijalne stvari. Računalni podaci u digitalnom obliku danas sve češće predstavljaju iznimno važnu imovinu. Štete koje nastanu oštećivanjem, izmjenjivanjem, brisanjem ili uništavanjem tuđih podataka mogu biti goleme.

Stavak 4. opisuje nezakonito presretanje kojim se traži sankcioniranje neovlaštenog presretanja nejavnih prijenosa računalnih podataka prema informacijskom sustavu, iz njega ili unutar njega (uključujući i elektromagnetske emisije iz informacijskog sustava koji prenosi te same računalne podatke) koje je počinjeno tehničkim sredstvom. Drugim riječima, to bi značilo da se ovim stavkom izričito zabranjuje prisluškivanje bežičnog prijenosa podataka te prisluškivanje žičanog prijenosa koje je moguće izvesti bez izravnog priključenja

[9] Šimundić, Slavko; Siniša Franjić: «Računalni kriminalitet», Sveučilište u Splitu – Pravni fakultet, 2009., str. 96. i 97.

na telekomunikacijsku liniju.

Stavak 5. uvodi kvalificirani oblik ovoga kaznenog djela kada je objekt radnje računalni podatak, program ili sustav tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnoga javnog interesa, ili je prouzročena znatna šteta, a što opravdano predviđa i težu propisanu kaznu. Ovdje se, kao mogući problem, može pojaviti određivanje „znatne štete".

Cilj kaznenopravne zaštite iz stavka 6. jest sprječavanje stvaranja i širenja tržišta naprava i u praksi vrlo čestih specijaliziranih programa za počinjenje kaznenih djela opisanih u stavcima 1., 2., 3. i 4. Inkriminacija tih kaznenih djela često se može provesti uz pomoć legalnih naprava i legalnih programa i tu se mogu pojaviti dodatni problemi.

Stavak 7. je poprilično jasan.

Stavak 8. kaže da Konvencija o kibernetičkom kriminalu u svom članku 11. stavak 2. traži da države potpisnice propišu kažnjavanje i za pokušaj kaznenih djela iz ovog članka, trebalo je izričito propisati i kaznu za pokušaj.

### 12. 2. Računalno krivotvorenje [10]

*Članak 223.a*

*(1) Tko neovlašteno izradi, unese, izmijeni, izbriše ili učini neuporabljivim računalne podatke ili programe koji imaju vrijednost za pravne odnose, u namjeri da se oni uporabe kao pravi ili sam uporabi takve podatke ili programe,*

*kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(2) Ako je kazneno djelo iz stavka 1. počinjeno u odnosu na računalne podatke ili programe tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa, ili je prouzročena znatna šteta,*

*počinitelj će se kazniti kaznom zatvora od tri mjeseca do pet godina.*

*(3) Kaznom iz stavka 1. ovoga članka kaznit će se tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1. ili 2. ovoga članka.*

*(4) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka oduzet će se.*

*(5) Za pokušaj kaznenog djela iz stavka 1. i 3. ovoga članka počinitelj će se kazniti.*

Stavak 1. kaže kako se u suvremenom gospodarskom poslovanju te u poslovanju

[10] Kazneni zakon NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08., 57/2011.

javne uprave i drugih pravnih osoba sve češće koriste elektroničke baze podataka te kako se brojne evidencije vode isključivo u elektroničkom obliku [11]. Mnoge od tih baza podataka imaju iznimnu vrijednost, a njihova izmjena, uništavanje ili brisanje čine takve podatke neuporabljivima. Oni mogu prouzročiti velike štete i predstavljaju veliku društvenu opasnost.

Stavak 2. implicira uvođenje kvalificiranog oblika kaznenog djela [12], a ovdje se također može pojaviti problem određivanja znatne štete.

Stavci 3., 4. i 5. su poprilično jasni.

### 12. 3. Računalna prijevara [13]

*Članak 224.a*

*(1) Tko s ciljem da sebi ili drugome pribavi protupravnu imovinsku korist unese, koristi, izmijeni, izbriše ili na drugi način učini neuporabljivim računalne podatke ili programe, ili onemogući ili oteža rad ili korištenje računalnog sustava ili programa i na taj način prouzroči štetu drugome,*

*kaznit će se kaznom zatvora od šest mjeseci do pet godina.*

*(2) Tko kazneno djelo iz stavka 1. počini samo s ciljem da drugoga ošteti,*

*kaznit će se kaznom zatvora od tri mjeseca do tri godine.*

*(3) Tko neovlašteno izrađuje, nabavlja, prodaje, posjeduje ili čini drugome dostupne posebne naprave, sredstva, računalne podatke ili programe stvorene ili prilagođene za činjenje kaznenog djela iz stavka 1. ili 2. ovoga članka,*

*kaznit će se novčanom kaznom ili kaznom zatvora do tri godine.*

*(4) Posebne naprave, sredstva, računalni podaci ili programi stvoreni, korišteni ili prilagođeni za činjenje kaznenih djela, a kojima je počinjeno kazneno djelo iz stavka 1. ili 2. ovoga članka oduzet će se.*

*(5) Za pokušaj kaznenog djela iz stavka 2. i 3. ovoga članka počinitelj će se kazniti.*

Stavak 1. kaže kako je ovdje bitan element pribavljanje protupravne imovinske koristi, a posljedica je prouzročenje štete drugome [14]. Pod ovo kazneno djelo moći će se svrstati razni oblici upada u računalne sustave sa svrhom promjene stanja na bankovnim računima, računalne prijevare s kreditnim karticama, plaćanja lažnim brojevima kreditnih kartica i sl. Tu također mogu spadati razne blokade računalnih sustava kako bi se onemogućila provjera valjanosti kartica, brisanje loše kreditne

[11] Šimundić, Slavko; Franjić, Siniša: Op. cit., str. 98

[12] Kvalifikatorne okolnosti mogu se odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice i sl.

[13] Kazneni zakon NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08., 57/2011.

[14] Šimundić, Slavko; Franjić, Siniša: op. cit., str. 98. i 99.

povijesti itd.

Stavak 2. kaže da se ovdje radi o privilegiranom obliku kaznenog djela [15]. Posljedica je i ovdje prouzročenje štete drugome, ali je cilj počinitelja da ošteti drugoga, odnosno cilj nije stjecanje protupravne imovinske koristi [16]. Određenu sličnu štetu čine kaznena djela iz članka 223. pa bi se u praksi moglo dogoditi da dođe do nedoumica pod koje kazneno djelo svrstati određeno ponašanje.

Stavci 3., 4. i 5. su poprilično jasni.

## 13. ZAKLJUČAK

Porastom broja korisnika Interneta, kako u svijetu, tako i u Hrvatskoj, sve se više širi i jedan od najpoznatijih pojavnih oblika računalnog kriminaliteta koji se naziva hoax.

Hoax je poruka elektroničke pošte neistinitog sadržaja poslana s ciljem zastrašivanja ili dezinformiranja primatelja. Hoax se javlja u nekoliko oblika kao što su upozorenja o štetnim programima, lanci sreće i zarade, lažni zahtjevi za pomoć, zastrašujući i prijeteći hoaxi, lažne peticije, kompromitirajući hoaxi te bezazleni hoaxi. Navedeni su primjeri za svaki od njih te je istaknuto kako prepoznati pojedinu vrstu. Širenje hoaxa u većini slučajeva ne može izazvati neku značajniju štetu, no, u određenim slučajevima hoaxa, hrvatsko kazneno zakonodavstvo, jednostavno, mora reagirati na način da se otkrije i primjereno kazni počinitelj.

## HOAX

The modern Information Society follow his numerous companions, of which one of the most dangerous computer crimes. The term “computer crimes” is considered the totality of crimes committed, which affects the unauthorized use, integrity and availability of technical, programming and data base computer system or the secrecy of digital information regardless of how much damage occurs due to them. Abuse of this kind are becoming increasingly common, and the consequences more dangerous. Given that modern computer technology every day more developed and accessible, we can say claim to almost the same speed and develop various kinds of abuse by her in today’s modern world should not be ignored. One of the most common method of manipulating computers is a hoax, e-mail messages that at first glance seem innocuous, but the possible consequences should not be considered negligible. This paper explains what a hoax, what are its consequences and legal protection under the Criminal law of the Republic of Croatia.

**Key words:** *Criminal Law, Convention on Cybercrime, Electronic mail, Computer crimes*

[15] Poput kvalifikatornih, i privilegirajuće se okolnosti mogu odnositi na modalitete radnje, svojstvo počinitelja ili objekta radnje, pobude, težinu posljedice itd. Za privilegirane oblike su propisane blaže kazne.

[16] Vojković, Goran; Štambuk-Sunjić, Marija: „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, 1/2006.

## 14. LITERATURA

1) www.infosecwriters.com / text_resources / pdf / Hoax_DCobaugh.pdf

2) www.carnet.hr

3) Šimundić, Slavko; Siniša Franjić: «Računalni kriminalitet», Sveučilište u Splitu – Pravni fakultet, 2009.

4) Kazneni zakon NN 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08., 57/2011.

5) Vojković, Goran; Štambuk-Sunjić, Marija: „Konvencija o kibernetičkom kriminalu i Kazneni zakon Republike Hrvatske“, Zbornik radova Pravnog fakulteta u Splitu, 1/2006.