ВИСОКА ПОСЛОВНА ШКОЛА
СТРУКОВНИХ СТУДИЈА – БЛАЦЕ
Часопис из области економије, менаџмента и информатике *„БизИнфо“*
Година 2014, годиште 5, број 2, стр. 57-65
Адреса: Краља Петра I, бр.70, 18420 Блаце

Прегледни рад

УДК: 343.451:004 ; 004.773.3

ZLOUPOTREBE ELEKTRONSKE POŠTE

ABUSIVE EMAIL

Vladica S. Ubavić[1]
Visoka poslovna škola strukovnih studija, Blace
Branislav P. Bogdanović[2]
Visoka poslovna škola strukovnih studija, Blace
Violeta J. Milićević[3]
Visoka poslovna škola strukovnih studija, Blace

Rezime: *Kada želimo da dobro i razumno objasnimo na koji način Internet radi i funkcioniše, nedvosmisleno naglašavamo da je to neformalan i jedan potpuno otvoren medij. Na Internetu informacije (podaci) slobodno teku i svakako ako slobodno teku svima su i dostupne, što ima za cilj da svako svoje informacije može i da plasira u svet. Potpuna i u pravom smislu reči Demokratija rekli bi mnogi. Međutim, nažalost Internet sve više liči na potpunu anarhiju. Sve je više korisnika interneta koji slobodu, odnosno anonimnost, koju pruža "globalna mreža" tumače na jedan sasvim pogrešan način. Takvi korisnici Interneta koriste internet servise na takav način da nanose veliku štetu, kako drugim internet korisnicicima, tako i velikim organizacijama i sistemima koji posluju na "mreži". Uzimajući u obzir značaj sigurnosti elektronske pošte, u ovom radu analizirani su negativni efekti zloupotrebe, kao i načini zaštite elktronske pošte.*
Ključne reči: *Elektronska pošta, spam, informacija, Int*

Abstract*: When we want to explain in a good and reasonable manner how the Internet operates and functions, we should clearly emphasize that it is a completely informal and open media. On the Internet, information (data) flow freely and if they are freely flowing and accessible, the aim is to for everyone*

[1]ubavic@vpskp.edu.rs
[2]bogdanovic@vpskp.edu.rs
[3]violeta.milicevic@vpskp.edu.rs

to be able to send their information to the world. Many would say that it is a true Democracy in every respect. However, unfortunately, it looks more like a complete anarchy. More and more Internet users interpret that freedom, or anonymity, which provides a "global network" in a completely wrong way. These people make use of the Internet services in such a way that inflicts major damage not only to other Internet users, but also to large organizations and systems that operate in the "network". Taking into account the importance of the security of electronic mail, the negative effects of abuse and ways of protecting Electronic junk mail are analyzed in this paper.
Key words: *Electronic mail, spam, Information, Internet*

1. UVOD

Kompjuterska tehnologija se danas može zloupotrebljavati na raznovrsne načine. Jedan od oblika zloupotrebe informacione tehnologije jesu računarske prevare. Predstavljaju najrašireniji vid kompjuterskog kriminaliteta, a imaju pretežno imovinski karakter (pribavljanje protivpravne imovinske koristi). Najčešće počnje pismom ili elektronskom porukom koja je tako osmišljena da izgleda kao da je namerno poslata primaocu poruke. U pitanju su lažne poruke o dobicimana igrama na sreću, dobrotvornim prilozima i dr. (Matijašević, Spalević i Ignjatijević, 2012, str. 562).

Elektronska pošta se naizgled možda čini kao pouzdan način konverzacije između dvoje ljudi, bezbedan od prisluškivanja trećeg lica, ali je isto toliko pouzdana koliko i šaputanje u školi. Vaša poruka može biti presretnuta bilo gde u putu između pošiljaoca i primaoca u bilo kom trenutku. Ukoliko šaljete e-mail sa posla, vaš šef može legalno da ima uvid u vašu elektronsku poštu, a ukoliko vaša firma u bilo kom trenutku bude pravno procesuirana, tužilac, ili strana koja vas tuži ima zakonsko pravo da preispita vašu elektronsku poštu, a vi zakonsku obavezu da im je date na uvid. Ako pošaljete e-mail od kuće, hakeri mogu da ga presretnu, ili ukoliko ste pod istragom nadležnih organa, isti mogu zapleniti elektronski zapis uz odgovarajući nalog. Čak i vaš internet provajder legalno može da kontroliše vašu elektronsku poštu. Sve u svemu na e-mail treba gledati kao na razglednicu, a ne kao na pismo.

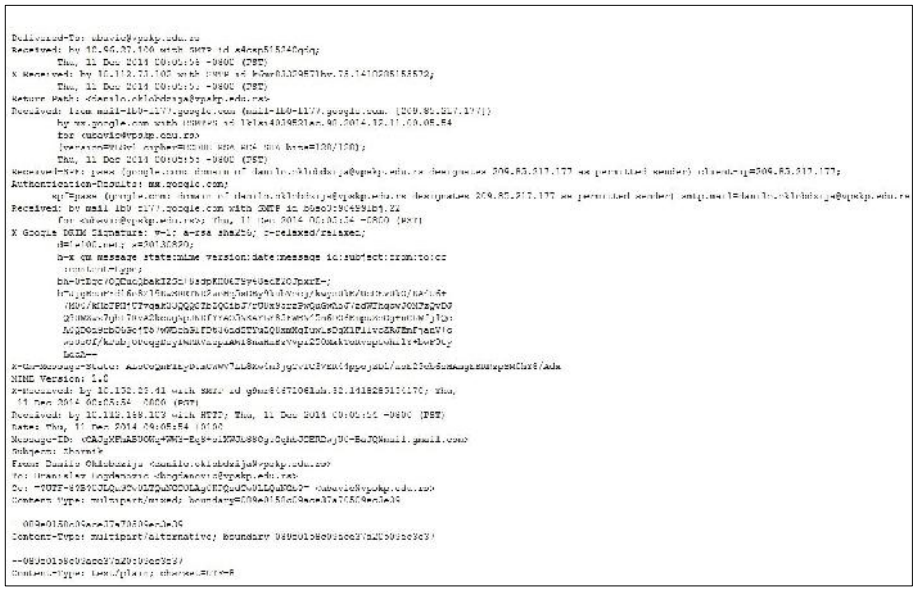
Pod zloupotrebom elektronske pošte**,** odnosno e-mail-a**,** mogu se smatrati sledeće aktivnosti (Microsoft 2014):

- prikupljanje i krađa ličnih i poslovnih informacija drugih korisnika elektronske pošte,
- zloupotreba podataka i propaganda u komercijalne svrhe putem elektronske pošte,
- lažno predstavljanje i krađa identiteta putem elektronske pošte
- korišćenje elektronske pošte kao načina distribucije zlonamernog softvera (raznih varijanti virusa, crva, trojanaca, keylogger-a …).

2. PRIKUPLJANJE I KRAĐA LIČNIH I POSLOVNIH INFORMACIJA DRUGIH KORISNIKA ELEKTRONSKE POŠTE (PERSONAL AND BUSINESS DADA ABUSE)

Generalno kršenje politike privatnosti korisnika je u pravom smislu reči kada se podaci o njima daju trećim licima bez njihovog izričitog odobrenja. Generalni problem kod elektronske pošte je u tome što ona u osnovi daje previše podataka o onome ko je tu poštu poslao. Iz nje se može saznati pre svega IP adresa pošiljalaca, a samim tim i odakle je poslata, iz koje republike, ko je pošiljalac, u koje vreme je poslata, preko kojih je sve servera prošla dok nije stigla do određene, odnosno krajnje destinacije.

Jako teško je izbeći kriminalne aktivnosti koje su vezane za samu elektronsku poštu, pošto je trenutno lako pratiti rad korisnika elektronske pošte programom za pristup pošti, raznim *sniff softverima*, probijati određenu zaštitu moćnim i vrlo lako dostupnim softverima.
Šifrovanje elektronskih poruka je dobra opcija (*Slika 1)*, ali ako neko stvarno želi da čita tuđe poruke, on može veoma lako da ih dešifruje sa odgovarajućim softverom za tu namenu.



Slika 1. Dobijene informacije iz pristigle elektronske pošte

3. ZLOUPOTREBA PODATAKA I PROPAGANDA U KOMERCIJALNE SVRHE PUTEM ELEKTRONSKE POŠTE (SPAM)

U klasičnu zloupotrebu elektronske pošte spada i takozvano "*spam*"-ovanje. To u suštini predstavlja slanje velikog broja jedne iste poruke velikom broju osoba, a od strane samo jednog pošiljaoca (najčešće su to neke vrste oglasa za proizvod ili uslugu koju pošiljalac želi da proda ili navede na prevaru).
Na taj način se osim zatrpavanja "mete" beskorisnim porukama, zauzimaju se resursi računara koji se koristi za slanje ili primanje tih poruka, pa moze doći i do blokiranja ili čak do oštećenja samog sistema.

U žargonu se nazivaju spamerima i mogu se podeliti u tri glavne kategorije:

- prva kategorija su oni koji svoju slobodu na Internetu koriste da se jednostavno zabavljaju na tuđ račun,
- druga kategorija su oni koji žele da ostvare neku vrstu dobiti, opet na tuđ račun, i
- treća kategorija, možda čak i najbrojnija kategorija su obični korisnici Interneta koji iz sopstvenog neznanja urade neke stvari koje nanose štetu drugima.

Naravno, samo se prve dve kategorije svrstavaju u štetne i one spadaju u grupu protiv koje se internet zajednica stvarno bori, jer samim tim što se bave takvim aktivnostima oni pokazuju svoju bezobzirnost i nepoštenje. Svi pokušaji da se neko od njih preobrati u normalne korisnike obično se završavaju potpuno bezuspešno. Oni su inače veoma maštoviti u nalaženju načina da maltretiraju što više ljudi ne prezajući ni od čega. Treća kategorija su tzv. “novajlije”. To su obični, normalni ljudi, koji nalaze Internet korisnim. Ipak, zbog svog neznanja umeju da naprave popriličnu štetu, i najčešće toga nisu ni svesni. U praksi, kada im se skrene pažnja oni se izvinjavaju i trude se da ne ponove greške.

Logično, kao odgovor na pojavu štetočina na Internetu su se pojavili i ljudi koji se bore protiv njih, antispameri. Ponekad stvarno izgleda da oni izigravaju dežurne policajce iako oni to nisu. Među njima prvenstveno spadaju administratori sistema. Bezobzirnost spamera je takva da uspeva čak i da podeli antispamere na umerene i bezobzirne. Razlika među njima je samo u tome što se ovi drugi ne libe da upotrebe sva raspoloživa sredstva u borbi protiv spamera, uključujući i ona koja se smatraju nelegalnim. Naravno, mi ne podržavamo korišćenje nelegalnih metoda u borbi protiv zloupotreba Interneta.

4. LAŽNO PREDSTAVLJANJE I KRAĐA IDENTITETA PUTEM ELEKTRONSKE POŠTE

Krađa identiteta je zločin kojim zločinci imitiraju druge ljude, obično za finansijsku dobit. U današnjem društvu, često se od pojedinaca traži da otkriju dosta ličnih informacija o sebi, kao što su brojevi socijalnog osiguranja, potpis, ime, adresu, telefonske brojeve, pa čak i informacije o bankarskim i kreditnim karticama. Ako je lopov u mogućnosti da pristupi ovim ličnim podacima, on ili ona može da ih iskoristi da počini prevaru u tuđe ime. Sa ovim informacijama lopov bi mogao da uradi stvari kao što su podnošenje zahteva za kredite ili nove račune kreditnih kartica. Zatim oni mogu zahtevati promenu adresa za obračun i koriste tuđu postojeću kreditnu karticu bez njihovog znanja. Oni takođe mogu da koriste falsifikovane čekove i kreditne kartice, ili da obave elektronske transfere u tuđe ime.

Ishod krađe identiteta je obično isti, bez obzira kako lopov dobija vaše informacije. Krađa identiteta na Internetu se razlikuje od obične krađe identiteta na nekoliko načina (Federal Bureau of Investigation 2013). Obična krađa identiteta se dešava nakon što je nekome nešto fizički ukradeno kao na primer novčanik sa kreditnim karticama i vozačkom dozvolom ili neiscepan izvod kreditne kartice iz kante za smeće. Lopov bi ove ukradene stvari koristio da napravi lažne kupovine u nečije ime ili nešto te prirode. Krađa identiteta na Internetu može biti mnogo gora. Krađa identiteta na Internetu može biti mnogo razornija nego konvencionalne krađe identiteta, jer je većina žrtava krađe identiteta na Internetu potpuno nesvesna da je nešto ukradeno od njih dok ne bude prekasno.

Krađa identiteta može da ide dalje od novčanih posledica. Lopovi mogu da koriste tuđe informacije da dobiju vozačku dozvolu ili neki drugi dokument na kome će biti njihova fotografija, ali tuđe ime i informacije. Sa tim dokumentima lopovi bi mogli da dobiju posao, podnesu zahtev za putne isprave, ili čak da učine da se i tuđe ime i poštanska adresa nađu u policiji i drugim organima ako je lopov uključen u druge kriminalne aktivnosti.

Dodatni način zloupotrebe elektronske pošte predstavlja slanje lažnih elektronskih poruka u žargonu "fake-mail"-ova. U pitanju je slanje poruka tako da izgleda da ih je poslao neko drugi. Najčešće se jedino iz zaglavlja poruke može otkriti da poruku nije poslao onaj čije ime piše u poruci, tako da ako ne očekujete suprotno, možete da pomislite da je poruku poslao onaj u čije je ime poslata.

Obično se šalje pošta sa identičnim logom i izgledom sajta za kojeg napadač želi da dobije pristup preko vaših pristupnih podataka. Obično je to npr. pošta

koja vas obaveštava da je njihova platforma zastarela i da će se uskoro ažurirati odnosno nadograditi i da ako se ne logujete u roku od 12 sati vaš nalog će se po automatizmu suspendovati. U takvoj elektronskoj pošti se ispod nalaze polja za unos podataka. Međutim, ti podaci se ne završavaju na pravoj strani već su vašim klikom na "ok" dospeli u ruke zlonamernom korisniku.

5. KORIŠĆENJE ELEKTRONSKE POŠTE KAO NAČINA PRENOSA-DISTRIBUCIJE MALICIOZNIH PROGRAMA (VIRUSA, CRVA, TROJANACA, KEYLOGGER-A)

Bombardovanje elektronske pošte je veoma primitivna tehnika, pa se gotovo više i ne koristi. Skoro svi provajderi imaju zaštitu od mail bombi. Zbog toga se koristi nova tehnika, a to je slanje e-maila koji može prouzrokovati veliku štetu. Radi se o slanju trojanca ili virusa uz e-mail u kojem se zlonamerni korisnik predstavlja kao veoma dobrotvorna osoba i neprimetno moli primaoca da startuje "program" koji mu je poslao (BackOrifice i NetBus su najpopularniji trojanci).
Pored trojanaca, opasnost predstavljaju i virusi koji se šire putem e-maila, tzv. crvi. Takvi virusi prate kome sve žrtva šalje poštu, i uz njihove e-mailove prikače i svoju kopiju, tako da primalac pošte dobije virus od svog prijatelja kome veruje.

Posebno treba obratiti pažnju na dva nova tipa crva, a to su crvi iz porodice tzv. "VBA crva" čiji je predstavnik sada već čuveni crv "I-LOVE'YOU" i crvi iz porodice "ActiveX crva" koju predstavlja crv "BubbleBoy".

6. POVEĆANJE STEPENA SIGURNOSTI PRILIKOM KORIŠĆENJA ELEKTRONSKE POŠTE

Sve su češći zahtevi da se elektronska poruka u prenosu ne može neovlašćeno pročitati, promeniti ili lažno generisati. U tu svrhu koriste se kriptografske tehnike za šifrovanje i digitalno potpisivanje (Boyd i Mathuria, 2003) čime se obezbeđuju tajnost i integritet podataka, kao i autentičnost subjekata u komunikaciji (Menezes *et al.*, 1996). Poruka se digitalno potpisuje kako bi lice na prijemu znalo da je ta poruka poslata od osobe sa kojom se vodi komunikacija. Drugoj strani se može verovati ukoliko iza nje stoji sertifikaciono telo (Ellison & Schneier, 2000).

Jedini način da obezbedite visok stepen privatnosti za poruke koje šaljete putem Interneta je da ih enkriptujete. Kodiranje je sistem u kome sofisticirani softver koristi kriptografske algoritme da šifruje vašu poruku, šalje je putem interneta kao niz besmislica do primaoca koji mora imati potreban softver za vraćanje poruke u prvobitnu formu. Najčešće se koristi tehnologija javnog

ključa (engl. Public key). Ova tehnologija koristi dva ključa, jedan koji je jedinstven i privatni, a drugi koji je javni. Ovi ključevi imaju funkciju samo kada su upareni. Ono što jedan ključ „promeša“(nasumično izmeša karaktere) samo drugi može da vrati u prvobitni oblik. Ova tehnika takođe proverava da li je poruka bila presretnuta i potvrđuje ko je zaista poslao poruku. Međutim, uspešno korišćenje enkripcije zahteva određeni nivo predviđanja, zato što osoba koja prima poruku mora biti u stanju da je i dešifruje. Dva popularna standarda enkripcije su Sigurna višenamenska ekstenzija za internet poštu (engl. Secure Multipurpose Internet Mail Extension) (S/MIME) i OpenPGP. Nijedan od ova dva softvera ne može da dekodira onaj drugi.

Softver PGP (engl. Pretty Good Privacy) već dugo važi za najsavršeniji u oblasti šifrovanja poruka. Njegov tvorac je amerikanac *Fil Zimerman*, (www.utexas.edu/its/secure/ articles/identity_ theft.php), koji je 1991. godine kreirao PGP i privukao veliki broj korisnika u vrlo kratkom roku.

PGP enkripcija koristi serijske kombinacije usitnjavanja i kompresije podataka i simetrično-kriptografske ključeve i javno-kriptografske ključeve. Svaki korak koristi jedan od nekoliko algoritama. Svaki javni ključ je vezan za korisničko ime i/ili e-mejl adresu (Federal Trade Commission, U.S. Department of Education 2010).

PGP se može koristiti za slanje poverljivih poruka. Za slanje ovakvih poruka PGP kombinuje simetrični-ključ za šifrovanje i javni-ključ za šifrovanje. Poruka je šifrovana pomoću simetričnog algoritma za šifrovanje koji zahteva simetrični-ključ. Svaki simetrični-ključ se koristi samo jednom i takođe se naziva ključ sesije. Sesijski ključ je zaštićen sa javnim-ključem primaoca čime se obezbeđuje da samo primalac može da dešifruje ključ sesije. Šifrovana poruka zajedno sa šifrovanim sesijskim ključem se šalje primaocu.

Karnivore je sistem implementiran od strane Federalnog istražnog biroa (FBI) koji je dizajniran za praćenje elektronske pošte i elektronskih komunikacija. On koristi prilagodljiv „sniffer“ paket za nadgledanje celog Internet saobraćaja ciljanih korisnika. „Carnivore“ je sproveden u oktobru 1997.godine, a 2005. godine je zamenjen sa poboljšanim komercijalnim softverom kao što je „NarusInsight“.

Prikupljanje informacija pružaoca usluga web pošte. Google, Hotmail, Yahoo kao i ostali web e-mail servisi mogu koristiti informacije o vama, o vašem računaru, identifikacionom broju vašeg modema kao i mnoge druge podatke iz više razloga. Jedan od razloga za takvu vrstu prikupljanja podataka je svakako unapređenje usluga datog servisa. Ostali su uglavnom vezani za vašu bezbednost prilikom korišćenja servisa. Policija može zatražiti od onoga ko pruža uslugu sve potrebne podatke ukoliko dođe do pokretanja istrage.

7. ZAKLJUČAK

Kako sve ima svoje prednosti i nedostatke, tako i Internet i računari sve više stvaraju neudoban i nepredvidljiv svet. Svako sredstvo za komunikaciju može se zloupotrebiti jer je sadržaj na internetu dostupan svima. Njihova nekontrolisana upotreba, kao i želja za zabavom, radoznalošću i naivnošću u znatnoj meri povećava rizik od zloupotrebe na internetu.

Elektronska pošta je jedna vrsta dokumenta koja se rangira kao dopis ili primljeni faks. U malverzacijama, pored toga što se uništavaju papirna dokumenta, uništava se i elektronska pošta kao važeći dokument i bitan dokaz za nezakonite radnje. Uzimajući u obzir važnost elektronske pošte, u ovom radu, ukazano je na mogućnosti ugrožavanja privatnosti, krađe identiteta i podataka, kao i na druge zloupotrebe, namerne ili nenamerne, i mogućnosti zaštite od istih.

REFERENCE

1. Boyd, C.A., Mathuria, A. 2003. *Protocols for Authentication and Key Establishment.* Berlin: Springer.
2. Beal, V., 2006. *How to Defend Yourself Against Identity Theft*. [online] (01.09.2006.) Dostupno na: <www.webopedia.com/DidYouKnow/Internet/identity_theft.asp> [Pristup 15.12.2014.].
3. Ellison, C., Schneier, B. 2000. Ten risks of PKI: What you're not being told about public key infrastructure. *Computer Security Journal.* 16(1), pp. 1-7.
4. Matijašević, J., Spalević, Z., Ignjatijević, S., 2012. Vrste internet prevara - pojam, značaj i uticaj na ekonomske i moralne aspekte društvene zajednice. *Međunarodni naučno-stručni simpozijum Infoteh-Jahorina.* Jahorina, Bosna i Hercegovina, 21-23 Mart 2012. Vol. 11, Mart 2012. Istočno Sarajevo: Elektrotehnički fakultet Istočno Sarajevo.
5. Menezes, A., Van Oorschot, P., Vanstone, S. 1996. *Handbook of Applied Cryptography.* New York: CRC Press.
6. Microsoft, 2014. *Email and web scams: How to help protect yourself.* [online] Dostupno na: <http://www.microsoft.com/security/online-privacy/phishing-scams.aspx> Pristup 16.12.2014.].
7. National Cyber Security Alliance. *ID Theft, Fraud & Victims of Cybercrime*. [online] Dostupno na: <http://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud> [Pristup 16.12.2014.].

8. Federal Trade Commission, U.S. Department of Education, 2010. *Preventing Online Identity Theft*. [online] Dostupno na: <http://www.utexas.edu/its/secure/articles/identity_theft.php> [Pristup 15.12.2014.].
9. Federal Bureau of Investigation, 2013. *Identity Theft.* [online] Dostupno na: <http://www.fbi.gov/about-us/investigate/cyber/identity_theft> [Pristup 15.12.2014.].

Рад је примљен 17.12.2014.
Прихваћен за објављивање 20.12.2014.