Komunikacija preko mreže: Spam, Internet interakcije i slanje poruka

Seminarski rad u okviru kursa
Metodologija stručnog i naučnog rada
Matematički fakultet

Bojanić Lazar, Dimović Đorđe, Filipović Marija, Stanojević Đorđe

6. april 2019.

Sažetak

Nagli razvitak Interneta doneo je nove mogućnosti, poput razgovora sa ljudima na drugom kraju sveta, automatskog paljenja svetla i grejanja kada pametan uređaj pomoću GPS-a zaključi da smo nedaleko od kuće i kupovine „iz fotelje". Pored pogodnosti, Internet je otvorio horizonte i akcijama koje izazivaju neprijatnosti i bezbednosne rizike, poput dobijanja neželjene pošte ili izlaganja korisnika reklamama koje bi ga potencijalno koštale sveg novca na bankovnom računu učini li samo jedan klik mišem. U radu autori objašnjavaju značenje i ulogu spama, njegov nastanak i istoriju. Rad govori i o načinima na koje spameri pronalaze svoje žrtve, i kako se korisnici Interneta mogu osigurati da ne budu među njima. Najzad, rad se bavi brojnim ulogama Interneta, objašnjavajuci na koje sve načine Internet može biti korisno i jednostavno sredstvo u ostvarivanju različitih ciljeva, od razonode do posla.

Sadržaj

1 Uvod

Svakog dana se u svetu preko aplikacije WhatsApp pošalje preko 65 milijardi poruka, preko 100 miliona glasovnih i 55 miliona video poziva koji zajedno traju oko 4 milijarde minuta [7].

Američki predsednik Donald Tramp je obavestio svojih 59.5 miliona pratilaca na Tviteru o postavljanju novog administratora u agenciji SBA i podelio novinski članak o izgradnji zida na američko-meksičkoj granici.

Internet i svi njegovi servisi su nam pružili nepresušan izvor informacija i mogućnost komunikacije u svakom trenutku. Ovo je, pored očiglednih olakšica u obavljanju svakodnevnih zadataka, vremenom dovelo i do stvaranja novih poteškoća. One variraju od nečega naizgled bezazlenog kao što je neželjena pošta, gde nam neko nudi proizvod koji ne želimo, preko narušene privatnosti, sve do kriminalnih aktivnosti kao što su prevare, Internet nasilje i krađe identiteta. U okviru ovog rada, autori se bave servisima koje nam Internet pruža i načinima na koje ti servisi i slanje tekstualnih poruka olakšavaju svakodnevnicu, ali i spamom, njegovim uticajem, razvojem i načinima borbe protiv njega.

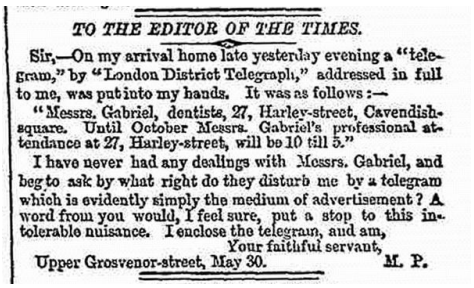
2 Spam

Poslednjih godina korišćenje elektronske pošte je u naglom porastu i postaje neizostavno sredstvo komunikacije sve većeg broja ljudi. Više od milijardu ljudi koristi e-poštu i svaki dan se pošalje oko 300 milijardi e-poruka. Nažalost, većina tih poruka su spam [5]. Spam definišemo kao masovne transmisije neželjenih poruka, odnosno to je poruka koja je poslata mnogim korisnicima e-pošte bez traženja njihovog odobrenja.

2.1 Nastanak i razvoj spama

Naziv je počeo da se koristi početkom 1990-ih godina i potiče od skeča Letećeg cirkusa Montija Pajtona, u kojem grupa vikinga u malom kafeu glasno viče „SPAM, SPAM, SPAM". Spam je konzervirano prerađeno meso koje se serviralo sa svakim jelom iz menija. Na ovaj način vikinzi ometaju razgovore drugih. Na sličan način spam poruke „guše" legitimne e-poruke [5].

Prva spam poruka je poslata 1864. godine pomoću telegrafa. Grupa britanskih političara dobila je telegram u kojim je saopšteno da će lokalna stomatološka ordinacija koju vodi gospođica Gabriel biti otvorena od 10 do 17 časova do oktobra.



TO THE EDITOR OF THE TIMES.

Sir,—On my arrival home late yesterday evening a "telegram," by "London District Telegraph," addressed in full to me, was put into my hands. It was as follows:—

"Messrs. Gabriel, dentists, 27, Harley-street, Cavendish-square. Until October Messrs. Gabriel's professional attendance at 27, Harley-street, will be 10 till 5."

I have never had any dealings with Messrs. Gabriel, and beg to ask by what right do they disturb me by a telegram which is evidently simply the medium of advertisement? A word from you would, I feel sure, put a stop to this intolerable nuisance. I enclose the telegram, and am,

Your faithful servant,

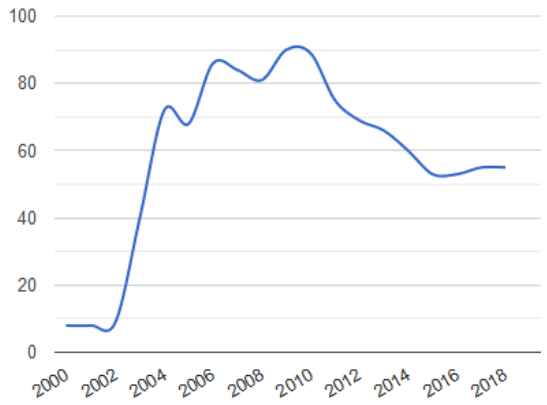
Upper Grosvenor-street, May 30. M. P.

Slika 1: Pismo žalbe koje je londonski list Times objavio 1864. godine

Prva spam poruka e-pošte poslata je 1978. godine kada je marketinški menadžer jedne računarske kompanije poslao poruku koja promoviše proizvode ove firme.

Komercijalni potencijal spama raste zajedno sa popularnošću Interneta. Grupa američkih advokata je 1994. godine preplavila grupe za diskusiju na USENET-u porukom koja je nudila pravne usluge imigrantima koji su se prijavljivali za zelene karte SAD-a. Masovno objavljivanje je izazvalo ogorčenje, ali taktika je donela više od 100.000 dolara prihoda, a moderna industija spama je rođena [4].

Spam poruke su 2000. godine činile samo oko 8% svih poruka. Uprkos tome, i dalje se smatrao problemom za pojedince koji su upravljali svojom poštom. Spam počinje da raste eksponencijalno, i do 2009. godine oko 90% svih poruka e-pošte su bile spam. Danas spam troši veliki procenat propusne moći Interneta i ogromne količine memorijskog prostora na mail serverima i sopstvenim računarima [5].



Slika 2: Zastupljenost spama u svim porukama u datom periodu

Imajući u vidu probleme koje spam može izazvati za svoje primaoce, poput izgubljenog vremena i truda, i izloženosti uvredljivim materijalima, prevarama i pretnjama, 2003. godine SAD su usvojile CAN-SPAM akt (Controlling the Assault of Non-Solicited Pornography and Marketing). Akt je uveden kako bi se utvrdili zakoni za one koji šalju komercijalne poruke, utvrdile kazne za pošiljaoce neželjene pošte i pružila prava potrošačima da traže od pošiljaoca da zaustavi slanje neželjenih poruka [8].

Tehnologija i tehnike koje služe za spamovanje i za blokiranje spam poruka se razvijaju velikom brzinom. Do 2018. godine procenat spam poruka je opao na 55%. Najveći procenat spam poruka su reklame, koje čine oko 36%. Na drugom mestu su spam poruke eksplicitnog sadržaja sa 31,7%, a na trećem poruke finansijskog sadržaja sa 26,5%. Prevare obuhvataju samo 2,5% svih spam poruka, međutim krađa indentiteta čini 73% ovog udela [8].

Glavna prednost spama u poređenju sa drugim oblicima reklamiranja je niska cena. Za između 500 i 2.000 dolara, kompanija može da pošalje reklamu na milion različitih adresa e-pošte. Poslati istu reklamu na milion kućnih adresa koristeći poštu košta najmanje 40.000 dolara, a 190.000 ukoliko je potrebno poslati na nasumične kućne adrese i sve to neuključujući troškove brošura. Drugim

rečima, reklama preko e-pošte košta 100 puta manje od tradicionalnog reklamiranja flajerima koji se šalju poštom [5].

Na svakih 12,5 miliona poslatih spam poruka, samo jedna osoba odgovori. To možda ne zvuči mnogo dok ne uzmemo u obzir da se preko 200 milijardi spam poruka šalje svakodnevno (prema podacima iz 2010. godine). Istraživanje je pokazalo da spamerima nije potrebna gomila odgovora kako bi zaradili. Čak i sa samo jednim odgovorom na 12,5 miliona poslatih poruka, spameri zarađuju oko 3,5 miliona dolara godišnje.

Spam poruke na nekoliko načina skupo koštaju kompanije širom sveta. Jedan od najočiglednijih načina je izgubljena produktivnost. Čak i ako se na spam potroši samo nekoliko minuta dnevno po zaposlenom, vreme koje zaposleni provede proveravajući ovakve poruke i ažurirajući filtere za spam može koštati kompanije na hiljade dolara tokom godine. Bombardovanje servera nizom spam poruka koje sadrže ogromne priloge može brzo zauzeti ogromne količine memorijskog prostora, a preuzimanje svih mailova na lokalni server, uključujući i spam, može izazvati smanjenje propusne moći Interneta.

2.2 Odbrana od spama

2.2.1 Spam filteri

U cilju zaštite primalaca od dobijanja neželjene pošte, široko su upotrebljene tehničke anti-spam mere. Razvijanje preciznih anti-spam mera je zahtevno sa tehničke strane, jer ne postoji precizna tehnička definicija spama koja se može iskoristiti u spam filterima. Problem je što spam po definiciji neželjene komercijalne elektronske pošte zavisi od stava primaoca prema primanju takvih poruka. Nevini pojedinci mogu biti uhvaćeni u unakrsnoj vatri između spamera koji razvijaju nove, sofisticiranije načine distribucije spam poruka, i anti-spam mera koje pokušavaju da otkriju spam poruke u cilju otklanjanja. To znači da potpuno legitimna elektronska pošta može biti pogrešno klasifikovana kao neželjena, ili se može zagubiti u poštanskom sandučetu gde je primalac neće primetiti.

2.2.2 Efekti anti-spam mera: zaštita korisnika i resursa

Primarni cilj anti-spam mera je smanjanje količine neželjene pošte. Poželjno je smanjiti količinu protoka Interneta posvećenog prosleđivanju neželjene elektronske pošte, međutim zadovoljstvo krajnjeg korisnika je daleko bitnije. Većina algoritama za filtriranje obrađuju informacije sadržane u telu poruke e-pošte, ali takođe mogu uzeti u obzir informacije sadržane u zaglavlju poruke (polja From, Subject, CC, itd.). Tipični primeri koji se koriste za smanjivanje spam poruka su odbijanje e-poruka sa terminima 'Free porn', 'XXX', 'Viagra', 'Get rich quick' i slično. Mnogi filteri koriste verovatnosni pristup poznatiji kao Bajesovsko filtriranje, gde svaka poruka e-pošte dobija ocenu na osnovu verovatnoće da se skup reči pojavi u neželjenoj pošti umesto u legitimnoj. Reči iz sadržaja poruke koje imaju vezu sa spamom, smanjiće ocenu elektronske poruke. Ako ocena poruke pređe određeni prag, smatraće se kao spam poruka i biće odbačena. Spam filteri mogu locirati poreklo poruke. Ako se poruka pošalje sa servera koji je od ranije poznat kao izvor spam poruka, povećava se verovatnoća da je i ta poruka kategorisana kao spam, i u nekim filterima ovo je dovoljno da se poruka klasifikuje.

Nijedna poznata tehnika nije potpuno rešenje za problem sa spamom, i svaka od njih ima kompromise između pogrešnog odbacivanja legitimne e-pošte, a neodbijanja spam poruka, i troškova u vremenu, naporu i ceni pogrešnog klasifikovanja. Anti-spam proizvodi često implementiraju kombinacije različitih tehnika filtriranja, blokiranja i učenja.

Tehnike koje zahtevaju akcije od strane pojedinaca - Postoje brojne tehnike koje pojedinci koriste da ograniče dostupnost svojih adresa e-pošte, sa ciljem smanjenja šansi za primanjem neželjene pošte. Jednostavna i efikasna tehnika za suzbijanje neželjene pošte su 'Ham' šifre [11]. Ham šifra je posebna lozinka koju tražimo od pošiljaoca da uključe u poruku koju nam šalju, na primer moguće je dodati takvu lozinku u zaglavlje poruke. Ako pošiljalac želi da korisnik primi poruku, mora uključiti jednu od korisnikovih lozinki kako bi dokazao da je ovlašćen da šalje elektronsku poruku. Ova tehnika je odlična u kombinaciji sa drugim tehnikama gde pojačava njihove slabosti. Ham lozinke mogu da otklone glavnu slabost heurističkih spam filtera, koji ponekad pogrešno kategorišu poruku. Ovaj pristup je jeftin, ne zahteva nikakve izmene u softverskom kodu i jednostavan je za razumevanje. Takođe je pod kontrolom korisnika, umesto da prepušta kontrolu nekom drugom. Ako imate lozinku, morate se pobrinuti da pošiljaoci mogu biti u stanju da je pronađu. Postoji mnogo načina da se to uradi; jedan od njih bi bio postavljanje šifre kao niza instrukcija, ili grafičke slike sa distorzijama. Na primer možemo postaviti instrukcije o tome kako se pravi lozinka: „prvo slovo je veliko 'L' iza čega sledi 'ozinka'".

Tehnike koje mogu biti automatizovane od strane administratora e-pošte - Postoji veliki broj aplikacija, uređaja, usluga i softverskih sistema koje administratori e-pošte mogu koristiti za smanjenje neželjenih poruka na svojim sistemima i u svojim poštanskim sandučićima. Uopšteno, ovo je pokušaj da se odbaci ili blokira većina spam pošte u fazi SMTP konekcije. Ako sistem prihvati poruku, obično će se onda dalje analizirati sadržaj - i mogu odlučiti da stave u karantin sve što je označeno kao neželjena pošta. Jedan od najranijih sistema za blokiranje neželjenih poruka su C/R sistemi (challenge/response) [10]. To su sistemi koji kada vide moguću neželjenu poštu od nekoga sa kime niste ranije komunicirali, privremeno blokiraju poštu i pošalju e-porukom „izazov" da bi pošiljalac potvrdio da je u pitanju osoba, a ne robot za slanje pošte ili spamer. Druga osoba dobija izazov i na neki određeni način odgovara na njega. Ako to uradi na ispravan način, sistem oslobađa poruku koja je blokirana, i od tada se mogu slati poruke bez izazova. Neki izazovi ukazuju na to da originalna pošta nije isporučena i od korisnika zahteva da je ponovo pošalje. Korisnici ovo mogu prihvatati sa dozom odbojnosti, specijalno ako smatraju da slanjem poruke čine uslugu primaocu (na primer odgovorili su na pitanje postavljeno na forumu), oni se često ne trude da ponovo pošalju poruku i odgovore na izazov. Zbog ovakvih situacija potrebno je učiniti izazov što jednostavnijim.

Kod filtriranja zasnovanom na poreklu poruke koristi se pristup blokiranja. Blokiranje znači da server e-pošte jednostavno odbija da prihvati bilo koju poštu sa određenih servera, često koristeći crne liste servera koje se dele na Internetu. Usluge kao što je Spamhaus Block List dozvoljavaju serverima e-pošte da u realnom vremenu provere da li je server koji pokušava da dostavi e-poštu dobio reputaciju spamera. Spamhaus Block List je baza podataka u realnom vremenu IP adresa spam izvora, uključujući poznate spamere, spam operacije i usluge koje podržavaju spam.

Zamke za spam (Spamtraps) su obično adrese e-pošte koje nisu kreirane za

komunikaciju, već za privlačenje neželjene pošte. Kako bi se sprečilo dostavljanje legitimne pošte, adrese e-pošte će se obično objavljivati samo na skrivenoj lokaciji, koju automatizovani sakupljači adresa e-pošte mogu pronaći. Budući da vlasnik ove zamka adrese ne očekuje bilo kakvu legitimnu poruku, svaka poruka poslata na ovu adresu se momentalno smatra nepoželjnom.

Tehnike koje mogu biti automatizovane od strane pošiljaoca e-pošte - Postoje razne tehnike koje pošiljaoci e-pošte koriste kako bi bili sigurni da ne šalju neželjenu poštu. Loše filtriranje poslatih poruka često može da dovede do blokiranja čak i legitimne e-pošte i da se pošiljalac stavi na crnu listu.

Pošto su nalozi elektronske pošte spamera često onemogućeni zbog kršenja pravila o zloupotrebi, oni stalno pokušavaju da kreiraju nove naloge. Zbog štete koju trpi ugled ISP-a kada je on izvor spama, mnogi ISP-ovi i dostavljač e-pošte koriste CAPTCHA na novim nalozima da bi potvrdili da je to čovek koji želi da napravi novi nalog, a ne automatizovani sistem za slanje neželjene pošte.

Zlonamerni softver i pošiljaoci spam poruka često falsifikuju polje FROM prilikom slanja spam poruka. Kontroli se može pristupiti na SMTP serverima da bi se osiguralo da pošiljaoci mogu da koriste samo njihovu ispravnu adresu e-pošte u FROM polju odlaznih poruka. U bazi podataka korisnika e-pošte svaki korisnik ima slog sa adresom e-pošte. SMTP server mora proveriti da li je adresa e-pošte u polju FROM odlazne poruke ista adresa koja pripada korisničkim podacima, isporučenim za SMTP autentifikaciju.

Tehnike koje angažuju službenike za sprovođenje zakona - Od 2000. godine, mnoge zemlje su usvojile specifično zakonodavstvo za kriminalizaciju spama, a odgovarajuće zakonodavstvo i sprovođenje zakona mogu imati značajan uticaj na aktivnost spamovanja.

Anti-spam napori su doveli do koordinacije između organa za sprovođenje zakona, velikih kompanija za finansijske usluge potrošača i dostavljača Internet usluga u praćenju spama, krađi identiteta, phishing aktivnostima i prikupljanju dokaza za krivične predmete.

Zakon o borbi protiv Internet i bežičnog spama je kanadski zakon protiv spama. Zakon nalaže da marketinški stručnjaci mogu slati samo e-poruke osobama koje se odluče za njihovo primanje. Takva saglasnost može biti implicitna, kao što je angažovanje u transakciji sa kompanijom, ili na osnovu toga što je telefonski broj ili adresa e-pošte navedena u javnom imeniku. Obavezno je da pošiljaoci omoguće primaocima da odustanu od primanja poruka. Ovim aktom je neophodno da marketinški stručnjaci šalju jednokratni zahtev za pretplatu svim pretplatnicima čiji pristanak nije izričito dat do dana stupanja na snagu ovog zakona.

2.2.3 Kako spameri sakupljaju adrese elektronske pošte?

U leto 2002. godine, CDT(Center for Democracy & Technology) je pokrenuo projekat kako bi pokušao odrediti izvor spama [2]. Napravili su stotine različitih adresa e-pošte, i svaku koristili za samo jednu svrhu, a zatim čekali šest meseci da vide kakvu vrstu pošte su primale te adrese. Mnoge adrese su privukle spam, i prikazani su različiti načini na koje adrese e-pošte privlače spam u zavisnosti od toga gde su korišćene.

Web stranice - CDT je primio najviše e-poruka kada je adresa bila posta-

vljena na vidljivom mestu na javnoj Web stranici. Spameri koriste programe kao što su „roboti" ili „pauci" za snimanje adrese e-pošte navedene na Web stranicama.
Testirane su dve metode ometanja robota pri skupljanju adresa:

- Zamena znakova u e-adresi ekvivalentim sadržajem čitljivim za ljude („primer@domen.com" bi bio napisan kao „primer at domen tacka com").
- zamena znakova u e-adresi pomoću HTML-a ekvivalenata

Sve adrese e-pošte koje su postavljene na javnu Web stranicu su dobile spam. Broj primljenih poruka je bio direktno povezan s popularnošću Web stranice. Nijedna od adresa koje su bile nejasne, bilo u „sadržaju čitljivom za ljude" ili „izmenjene dodatnom HTML formom", nije primila ni jedan spam.

USENET grupe – Grupe za diskusiju mogu spamerima prikazati e-adresu svake osobe koja nešto objavi u diskusionoj grupi, i one su posle Web stranica privukle najviše spam poruka. Iako generišu manje neželjene pošte nego postavljanje adrese e-pošte na web stanicu, 85% adresa je primilo spam.

Davanje adrese e-pošte web kompanijama - Treća oblast koja je testirana bila je do kog stepena su Web kompanije poštovale odluku potrošača da odustanu od primanja komercijalne e-pošte. U svim slučajevima gde je podeljena adresa e-pošte i gde je pitano da se više ne prima komercijalna e-pošta, Web stranice su ispoštovale taj zahtev - nisu dobijene spam poruke nakon toga.

WHOIS baza - Kada korisnik registruje ime domena u jednom od sedam globalnih domena Interneta ili određenih domena najvišeg nivoa zemlje, njegove kontakt informacije se unose u javno dostupnu bazu podataka poznatu kao WHOIS baza podataka. Testirano je koliko će spama biti primljeno na navedenoj adresi u WHOIS bazi podataka i samo jedna spam poruka je primljena u toku šest meseci projekta.

Zanimljivo je što je u jednom trenutku sistem za poštu počeo da prima spam poruke na adrese koje se nikada nisu postojale. Utvrđeno je da je sistem bio žrtva „brute force" napada u kojem je spamer pokušao da pošalje e-poruke na sve moguće kombinacije slova koja mogu formirati adresu e-pošte.

3 Internet interakcije

Internet, odnosno 'mreža svih mreža', danas povezuje milijarde računara, telefona, tableta i drugih pametnih uređaja širom sveta. Međutim, Internet ne predstavlja samo rezultat tehnološkog napretka. Naime, ova mreža koja funkcioniše bez centralizovanog uređenja, i sa nehijerarhijskom organizacijom takođe je značajna za društvene i političke procese, naučnu zajednicu, trgovinu, poslovanje, humanitarne organizacije, itd. Internet se sastoji od miliona manjih kućnih, akademskih, poslovnih, vladinih, i drugih mreža, koje međusobno razmenjuju informacije i korisnicima nude usluge poput korišćenja World Wide Weba, četovanja, prenosa datoteka, razmene elektronske pošte, i mnoge druge.

3.1 Veb

Važan uticaj na promenu Interneta u odnosu na njegove početke imao je ogroman porast broja korisnika usled pojavljivanja World Wide Web-a. Kreiran je od strane Tima Berners-Lija prvenstveno kao dokumentacioni sistem za CERN, koji je za cilj imao da mnoštvo ljudi podeljenih u razne timove imaju pristup uvek najnovijim podacima istraživanja koje mogu menjati. Međutim jednostavnost korišćenja Veba omogućila je da on bude dostupan i svim ostalim običnim korisnicima računara. Veb čini mnoštvo veb stranica u kojima nailazimo na veze ka drugim stranicama, što nazivamo hipertekstom. Za posete ovim veb stranicama koristimo pretraživače veba kao što su Google Chrome, Mozilla Firefox, Opera, Safari, i druge. Dve osobine veba koje su omogućile da veb postane glavno sredstvo razmene informacija jesu njegova decentralizovanost - pojedinac može dodati novi sadržaj bez dozvole centralnog autoriteta i jedinstvenost adrese svakog objekta, čime se jedan objekat može povezati sa drugim korišćenjem samo te adrese [9].

3.2 Aplikacije

Iako je korišćenje veb pretraživača jednostavno na računarima i laptopovima, ono može biti nezgodno u slučaju pametnih telefona, tablet računara i drugih mobilnih uređaja. Međutim, ljudi sve više koriste ove mobilne uređaje, zbog čega je doslo do razvijanja mobilnih aplikacija, odnosno softvera za rad na mobilnim uređajima. Aplikacije mogu biti već prethodno instalirane na uređaju, ili se mogu naknadno instalirati upotrebom distributivnih platformi njihovih proizvođača, poput App Store aplikacije za Apple uređaje, ili Play Store aplikacije za Android. Korišćenje aplikacija se moze naplaćivati, ali one mogu biti i besplatne. Aplikacije rade kao samostalni programi, ili zahtevaju Internet konekciju i omogućavaju učitavanje i preuzimanje podataka sa veba. Prvobitno su se aplikacije koristile u svrhu razmene elektronske poste, ali je s porastom njihove potražnje došlo do razvoja velikog broja aplikacija koje nude raznovrsne usluge korisnicima u različite svrhe.

3.3 Za šta koristimo Internet

Zahvaljujući veb pretraživačima i mobilnim aplikacijama Internet je dostupan ljudima koji nisu prošli kroz računarsku obuku i nemaju iskustva u radu na računaru. Kao rezultat toga, danas milioni ljudi pristupaju Internetu svakodnevno u različite svrhe.

Internet kupovina i plaćanje računa - Korisnici imaju mogućnost elektronske kupovine robe ili usluga prodavca preko Interneta korišćenjem veb pregledača. Potrošači mogu vršiti elektronsku kupovinu preko stonih ili laptop računara, pametnih telefona i tableta. Veb sajtovi prodavaca ili organizacija omogućavaju pregled i naručivanje robe ili usluga iz udobnosti naših domova, ali i na bilo kojoj drugoj lokaciji, jedino što je neophodno jeste pametan uređaj sa ostvarenom Internet konekcijom. Zahvaljujući Internetu moguće je plaćati račune na brz i jednostavan način. Platilac moze putem Interneta preneti određenu svotu novca sa svog računa ili kreditne kartice na račun prodavca, pružioca usluge, javnog servisa ili robne kuce, i uštedeti sebi vreme i trud.

Društvene mreže - Internet je postao popularno i jednostavno sredstvo za održavanje kontakta među ljudima. Postoji mnogo načina za sticanje novih poznanstava i održavanje postojećih društvenih odnosa na Internetu. Jedan od prvih načina komunacije preko Interneta je bio putem elektronske pošte. Pored elektronske pošte, danas je moguće razmenjivati i instant poruke, što predstavlja brži vid razmene poruka, audio poruke, ili vršiti video pozive u slučaju potrebe za vizuelnom komponentom pri komunikaciji. Zanimljivo je da se video pozivi posredstvom neke od aplikacija koje nude ovakvu uslugu, poput aplikacije Skype, koriste ne samo radi razonode u krugovima prijatelja i porodice, već i u poslovnom svetu, za vršenje video konferencija. Forumi su veb sajtovi pomoću kojih ljudi zajedničkih interesovanja mogu međusobno da komuniciraju. Sobe za četovanje daju mogućnost Internetu i komunikacije sa njima, prilikom čega korisnici mogu da upoznavanja ljudi na ostanu anonimni, što može biti pogodno u slučaju da korisnik želi da sakrije svoj identitet iz bezbednosnih razloga, ali s druge strane i rizično, budući da korisnik ne moze znati s kim komunicira s druge strane veze. Razvoj tehnologije praćen je razvojem novih načina komunikacije preko Interneta. Nezaobilazna pojava u novoj eri su društvene mreže, koje omogućavaju ne samo razmenu instant poruka, već i deljenje tekstualnih, slikovnih, video sadržaja sa drugim korisnicima mreže, kao i komentarisanje podeljenih sadržaja drugih ljudi. Društvene mreže funkcionišu kao online društvene zajednice, koje omogućavaju ljudima iz istih društvenih krugova laku komunikaciju i saznanje o aktivnostima njihove porodice i prijatelja, ali isto tako one mogu biti i sredstvo za sticanje novih poznanstava. Neke od najviše korišćenih društvenih mreža su Facebook, YouTube, Instagram i QZone [3].

Naziv mreže	Broj korisnika u milionima	Vrednost kompanije	Prosečno korišćenje po danu
Facebook	2 271	$434 milijardi	35 minuta
Whatsapp	1 500	u vlasništvu Facebook-a	45 minuta
Instagram	1 000	u vlasništvu Facebook-a	44 minuta
Reddit	330	$2,7 milijardi	55 minuta
Twitter	326	$13 milijardi	35 minuta
Linkedin	303	$27 milijardi	12 minuta

Tabela 1: Društvene mreže

Wiki - Pored društvenih mreža, mogućnost postavljanja novog sadržaja na veb nude i druge vrste veb stranica. Wiki prestavlja veb sajt koji omogućava mnoštvu korisnika postavljanje novog, i menjanje postojeceg sadržaja sajta. Najpoznatija wiki jeste Wikipedia, besplatna elektronska enciklopedija, jedna od najvećih enciklopedija na svetu. Wikipedia sadrži članke na više od četvrdeset različitih jezika, od čega svaki ima bar po 100,000 članaka []. Engleski jezik je najčešće korišćeni jezik za pisanje članaka, sa 5,836,709 napisanih članaka u trenutku pisanja rada []. Autori članaka su dobrovoljci, koji po želji mogu navesti svoj identitet, koristiti pseudonim ili ostati anonimni. Wikipedia ima svoja pra-

vila i polise u cilju unapređenja enciklopedije, ali se od dobrovoljaca nužno ne zahteva da budu upoznati s njima. Međutim, često se poteže pitanje o kvalitetu ovih članaka, budući da bilo ko sa pristupom Internetu može da ih postavi na Wikipediu.

Blogovanje - Korisnici ne moraju samo koristiti veb za preuzimanje sadržaja, već ga mogu korisiti i u svrhu građenja društvenih zajednica i deljenja svojih sadržaja. Blog je lični dnevnik koji je smešten na vebu. Aktivnost održavanja takvog dnevnika redovnim postavljanjem novog sadržaja naziva se blogovanje. Blog moze sadržati tekst, slike, audio ili video snimke. Primeri blogova su Blogspace i Livejournal. Veb zajednice poput ovih imaju određena nepisana pravila ponašanja, na primer, korisnici blogova neće težiti da otkriju identitet autora ukoliko on želi da ostane anoniman. Međutim, ima korisnika koji se s namerom ponašaju neprikladno u ovakvim zajednicama, takozvani „trolovi". Bezbednost na Internetu je prioritet nekih veb sajtova, gde se ne toleriše diskriminacija, i od korisnika se zahteva isticanje obaveštenja u slučaju postavljanja sadržaja koji bi mogli biti uznemirujući za druge, poput onih koji obuhvataju neki vid nasilja ili mogu biti štetni po ljude koji boluju od epilepsije.

Edukacija - Internet predstavlja sastavni deo obrazovnog sistema u razvijenim državama. Profesori koriste Internet kao sastavni deo svojih predavanja, i univerziteti širom sveta postavljaju materijale za učenje i online kurseve na svoje veb stranice. Postoji i mogućnost održavanja časova preko Interneta, što se ostvaruje putem video poziva, ili deljenjem video zapisa, a rezultira u uštođenom vremenu i novcu. Internet sadrži mnoštvo korisnih podataka, naučnih članaka, elektronskih knjiga i enciklopedija, kojima se može brzo pristupiti. Upravo ove odlike Interneta su dovele do toga da on u modernom dobu zameni biblioteke kao mesto u pravcu kojeg se usmerimo pri traženju materijala za učenje ili prikupljanje informacija.

Igrice - Online igrica je igrica koja se igra na računarskoj mreži koja podržava simultano učešće više igrača. Trajna online igrica je online igrica u kojoj svaki igrač preuzima ulogu karaktera iz virtuelnog sveta i odlike karaktera i virtuelnog sveta postoje i izvan pojedinačne igre. Virtuelni svet je računarski stvorena simulirana sredina koja je dostupna korisnicima koji naprave ličnog avatara, i zatim simultano i nezavisno istražuju virtuelni svet, učestvuju u njegovim aktivnostima i komuniciraju sa drugim korisnicima. Avatari su uglavnom dvodimenzionalni ili trodimenzionalni grafički prikazi. Velike online igrice za više igrača prikazuju širok spektar virtuelnih svetova, zasnovanih na naučnoj fantastici, superherojskim motivima, sportu, horor pričama, istorijskim događajima ili realnom svetu. Jedna od popularnih trajnih online igrica je World of Warcraft. Senzacija online igrica dovela je do toga da učešće u ovakvim igricama postane izvor prihoda, odnosno proizvela je profesionalne igrače online igrica.

Internet of Things - Internet of Things (IoT) je sistem međusobno povezanih računarskih uređaja, mehaničkih ili digitalnih mašina, objekata, životinja ili ljudi kojima su pridruženi jedinstveni identifikatori i sposobnost prenosa podataka putem mreže bez potrebe za međusobnom interakcijom između ljudi ili između računara i čoveka. Veliki broj uređaja - termostati, svetla, senzori za kretanje, bezbednosni sistemi za kuće, kamere, brave na vratima, monitori za bebe

itd., pomoću dostupne bežicne Internet konekcije mogu biti kontrolisani i nadzirani od strane ljudi preko veb pregledača, čak i sa velikih razdaljina. Pojedini uređaji sa Internet konekcijom mogu biti programirani tako da vrše međusobnu interakciju bez ljudskog nadzora. Pametni uređaji su zaslužni za veću efikasnost u mnogim profesionalnim oblastima. U proizvodnji senzori ugrađeni u radnu opremu mogu da utiču na smanjenje vremena potrebnog za proizvodnju i količine dobijenog otpada. Takođe, senzori mogu da utiču na smanjenje broja preventivnih pregleda mašina predviđajući period u kojem će mašinama biti potrebno održavanje, čime se smanjuju novčani troškovi i količina utrošenog vremena. IoT doprinosi i uštedi energije, korišćenjem senzora koji kontrolišu osvetljenje, temperaturu i upotrebu električne energije u domu. Pametni termostat može automatski da isključi grejanje ili hlađenje kada za njim nema potrebe kako bi uštedeo energiju. U slučaju poljoprivrede, senzori bi mogli na osnovu vlažnosti zemljišta i vremenske prognoze da navodnjavaju zemljište samo onda kada je to potrebno, čime se smanjuje količina potrošene vode. Pametni uređaji imaju značajnu ulogu i u brizi o starim licima i deci, predviđanjima prirodnih katastrofa, sprovođenju zakona i povećanju kvaliteta životne sredine.

4 Slanje poruka

Porast broja korisnika društvenih mreža doveo je do toga da se one mogu koristiti i u marketinške svrhe. Preduzeće ili pojedinac moze napraviti profil na nekoj od društvenih mreža i potom se na njemu oglašavati o svojoj poslovnoj ponudi. Prednosti ovakvog načina oglašavanja jesu prvenstveno dvostrana komunikacija, koja kod tradicionalnog oglašavanja putem nekog medija kao što su novine ili televizija ne postoji[6]. Na ovaj način je oglašivač u mogućnosti da neposredno komunicira sa klijentom uzimajući u obzir njihove predloge i mišljenja. Još jedna prednost i razlog zbog kojih je ovaj način komunikacije u porastu je cena. Postavljanje sadržaja na mreže je besplatno, što pogoduje razvoju malih preduzeća koja nemaju sredstva za tradicionalni pristup [5].
Kao jedan od primera poslovne promocije može se uzeti belgijska pivara Maes, koja je napravila kampanju u kojoj svaka osoba koja ih kontaktira, a da se preziva Maes dobija bure njihovog piva pod uslovom da pivo podele sa dvadeset prijatelja. Vest se proširila zahvaljujući društvenim mrežama, i akcija je rezultovala dobijanjem 100,000 novih pratilaca na njihovoj Fejsbuk stranici, i preko 500,000 poseta. Takođe, 7,000 ljudi promenilo je prezime u Maes na Fejsbuku kako bi učestvovali u akciji [1].

Korisnici društvenih mreža imaju slobodu da putem mreža iznose svoje životne stavove i uverenja. Zbog ovoga se neretko dešava da se slanjem poruka i deljenjem objava na društvenim mrežama međusobno pronalaze istomišljenici, i da se upravo putem društvene mreže vrši organizacija javnih skupova i dešavanja. Ovakav način komunikacije imao je važnu ulogu u zbacivanju sa vlasti filipinskog predsednika Josefa Estrade 2001. godine. Estradini politički saveznici u filipinskom kongresu su izglasali da se ne otkriju neki od inkriminišućih dokaza u tada aktuelnom suđenju. U narednim danima, Filipinci su slali jedni drugima milione poruka o protestnim okupljanjima, koja su postala toliko masovna da je kongres promenio svoju odluku i objavio dokaze [5].

5 Zaključak

Osnivač Microsoft-a Bill Gates izjavio je 2004. godine da će problem sa spam porukama biti rešen u naredne dve godine. Četrnaest godina kasnije uprkos velikim naporima, borba protiv spama je i dalje prisutna. Spam je ozbiljan problem mnogim korisnicima usluga e-pošte, i mnogo istraživanja iz oblasti anti-spam mera je urađeno poslednjih godina. Usled same distribuirane arhitekture Interneta, teško je napraviti anti-spam meru sa stoprocentnom preciznošću. U radu smo predstavili nekoliko metoda anti-spam mera, i zaključili da je trenutno najveći problem automatsko skupljanje adresa e-pošte sa javno dostupnih veb stranica. Takođe smo primetili da je metod izmene adrese e-pošte u formu čitljivu ljudima za sad jako dobro rešenje. Osvrnuli smo se na neke od korisnih usluga Interneta, i primetili da nam njegovo korišćenje sve više čini deo svakodnevnice. Prikazana je svestranost društvenih mreža i njihove primene za marketinške svrhe, gde je ukazano na ogroman potencijal koje one donose.

Literatura

[1] Chris Cloutier. 30 Businesses that Are Rocking Social Media, 2018. on-line at: https://smallbiztrends.com/2014/07/best-social-media-marketing-examples.html.

[2] Center for Democracy & Technology. Unsolicited Commercial E-mail Research Six Month Report, 2003. on-line at: https://www.spamhelp.org/articles/030319spamreport.pdf.

[3] PRIIT KALLAS. Top 15 Most Popular Social Networking Sites and Apps, 2018. on-line at: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/r.

[4] The Editors of Encyclopaedia Britannica. Spam, 2019. on-line at: https://www.britannica.com/topic/spam.

[5] Michael J. Quinn. *Ethics for the information age*. Pearson, 2015.

[6] Mahmud Akhter Shareef. Social media marketing: Comparative effect of advertisement sources. 2019. on-line at: https://www.sciencedirect.com/science/article/pii/S096969891730591X.

[7] Craig Smith. WhatsApp Statistics and Facts, 2019. on-line at: https://expandedramblings.com/index.php/whatsapp-statistics/.

[8] David E. Sorkin. Spam Laws. on-line at: https://www.spamlaws.com.

[9] Andrew S. Tanenbaum and David Wetherall. *Computer networks, 5th Edition*. Pearson, 2011.

[10] Brad Templeton. Proper principles for Challenge/Response anti-spam systems, 2003. on-line at: https://www.templetons.com/brad/spam/challengeresponse.html.

[11] David A. Wheeler. Countering Spam by Using Ham Passwords (Email Passwords), 2011. on-line at: https://dwheeler.com/essays/spam-email-password.html.