Godina IV | Broj 8 | Sveska 2/2016 | ISSN 2334-816X

TRENDOVI U POSLOVANJU
NAUČNO-STRUČNI ČASOPIS

PRIVATNOST NA INTERNETU – MIT ILI REALNOST

PRIVACY IN THE INTERNET – MYTH OR REALITY

Bratislav Mikarić, spec., Visoka poslovna škola strukovnih studija "Prof. dr Radomir Bojković" Kruševac, bratislav.mikaric@indmanager.edu.rs

Marija Marković, MA, Visoka škola za poslovnu ekonomiju i preduzetništvo, Beograd, marija.markovic@indmanager.edu.rs

Mr Dušan Trajković, Visoka poslovna škola strukovnih studija "Prof. dr Radomir Bojković" Kruševac, dusan.trajkovic@indmanager.edu.rs

Sažetak

U današnje vreme koje je nezamislivo bez korišćenja interneta – od imejla, preko društvenih mreža, cloud servisa, GPS-a, pa do jutjuba i mobilnog računarstva, kako na poslovnom, tako i na privatnom planu, postavlja se pitanje da li uopšte postoji mogućnost zaštite privatnosti podataka na internetu. Koji su načini da kontrolišemo šta ćemo od ličnih podataka javno deliti sa drugima i da li postoji siguran način za zaštitu privatnosti na svetskoj globalnoj mreži računara? U radu je dat pregled stanja u navedenoj oblasti, kao i saveti za postizanje željenog nivoa zaštite podataka.

Abstract

The present time, unthinkable without using Internet - from e-mail, through social networks, cloud services, GPS, to YouTube and mobile computing in business, as well as on a private level, poses a question:" Is there a way to protect data and their privacy on the Internet? What are the ways to control what personal information we will publicly share with others and is there a safe way to protect privacy on the world's global computer network? The paper gives an overview of the situation in the field, as well as tips for achieving the desired level of data protection.

Ključne reči: *privatnost, bezbednost, zaštita, podaci, internet*

Keywords: *privacy, security, protection, data, Internet*

1. Uvod

Svima je jasno da na internetu nema baš mnogo privatnosti. Naravno, postoje ljudi kojima ovo nije bitno i koji bez problema dele svaki svoj privatni momenat na društvenim mrežama, ali postoje i oni koji žele da sačuvaju svoju privatnost na internetu.

Definicija - Šta internet privatnost predstavlja?

Internet privatnost je nivo privatnosti i bezbednosti ličnih podataka objavljenih putem interneta. To je širok pojam koji se odnosi na različite faktore, tehnike i tehnologije koji se koriste za zaštitu osetljivih i privatnih podataka, komunikacija i preferencija.

Privatnost na internetu i anonimnost su najvažniji za korisnike, posebno u oblastima kao što je e-trgovina i ta pitanja nastavljaju da privlače pažnju. Povrede privatnosti i rizici krađe podataka su standardna razmatranja za bilo koji ozbiljan sajt u razvoju.

Internet privatnost je takođe poznata i kao onlajn privatnost. [1]

2. Šta se sve zna o korisniku interneta

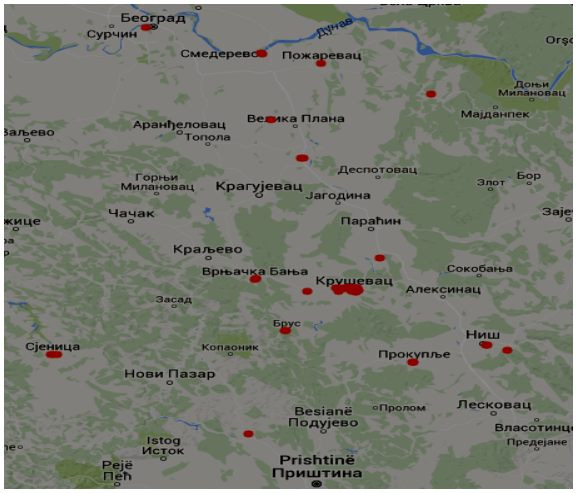
2.1. Interesovanja i demografski podaci

Guglu je veoma stalo da zna što više o vama. On želi da zna koliko godina imate, vaš pol, gde živite itd. i prati stranice koje posećujete kako bi procenio vaša interesovanja, a sve to sa ciljem da vam prikaže oglase za koje smatra da vas zanimaju. Treba pomenuti da Gugl ne krije

(od Vas) koja su vaša interesovanja i ukoliko ste ulogovani u *Google Chrome*, možete lako videti koja interesovanja vam je dodelio (i izbaciti netačna interesovanja). Samo ukucajte u pretraživač "*Google ads settings*" i izaberete "*Interests*" kategoriju.

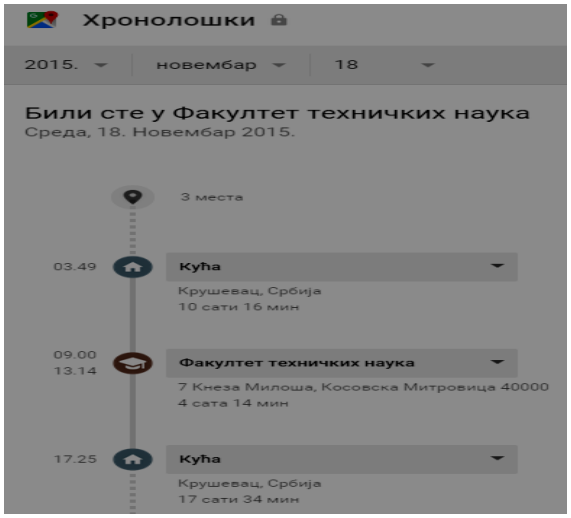
2.2. Istorija kretanja

Ukoliko Vaš telefon koristi Android operativni sistem i ako ste uključili opciju istorije kretanja, slaće podatke Guglu o vašem kretanju. Tako pomoću njega možete videti gde ste sve bili određenog dana, kojom ste se brzinom kretali i sl. Sve što treba da uradite je da u Gugl ukucate "*Google location history*".



Slika 1. Prikaz praćenja lokacije putem Android pametnih telefona, Izvor: autor

Ne samo da ćemo dobiti putanju kretanja, već i prilično precizno vreme i lokacije na kojima smo bili, zajedno sa trajanjem naših poseta, kao što je prikazano na slici 2.



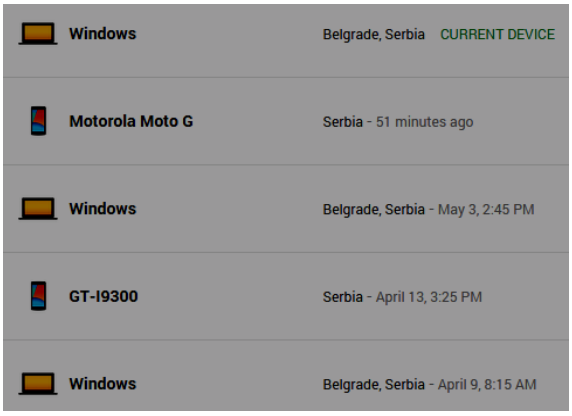
Slika 2. Prikaz praćenja kretanja sa vremenima putem Android pametnih telefona, Izvor: autori

2.3. Istorija pretraga na Guglu

Pretpostavimo da ste neki sajt našli preko Gugla, ali ne možete da se setite koju frazu ste koristili prilikom pretrage i ne možete da ga nađete u istoriji poseta. Srećom, on već pamti sve upite, tako da je dovoljno da ukucate "*Google history*" i prikazaće vam se stranica sa svim pretragama koje ste izvršili.

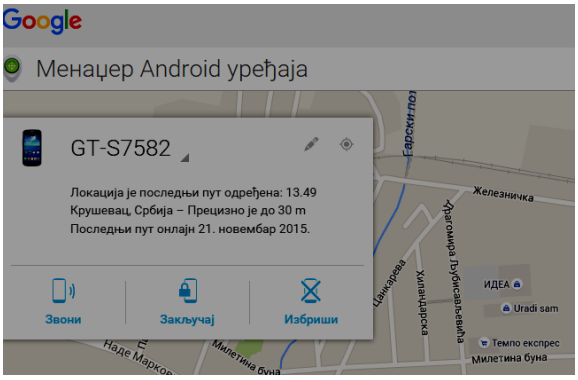
2.4 Uređaji koji su korišćeni za logovanje na Gugl nalog

Ako sumnjate da je neko koristio vaš nalog, to možete lako proveriti. Dovoljno je samo da ukucate "*Google devices and activity*" i prikazaće vam se svi uređaji koji su se povezivali na vaš nalog, njihova IP (*Internet Protocol)* adresa i okvirna lokacija.



Slika 3. Prikaz uređaja preko kojih se korisnik prijavljivao na Google nalog, Izvor: autori

I više od toga, vrlo jednostavno se može dobiti i model telefona kojim je pristupljeno, sa koje lokacije, sa prilično tačnošću od 20-30m, datumom i vremenom pristupa, kada je uređaj poslednji put bio na mreži, ali i korisnim mogućnostima da taj uređaj zaključate (ukoliko ste ga pre toga registrovali i vezali za svoj imejl nalog), izbrišete sa liste svojih uređaja ili da ga inicirate da zvoni neprekidno par minuta, kao i da mu zaključate ekran sa tasterom za pozivanje broja koji odredite i porukom koja se ispisuje na zaključanom ekranu, kao što je prikazano na slici 4.



Slika 4. Prikaz uređaja preko kojieg se korisnik prijavljivao na Google nalog sa detaljima, Izvor: autori

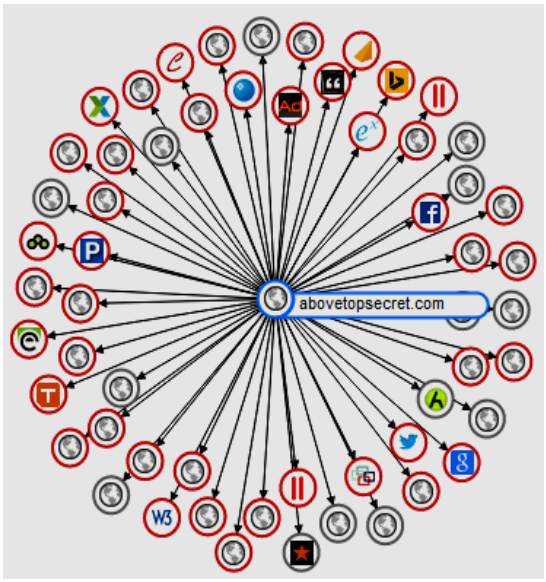
2.5. Izvlačenje podataka

Ako na Guglu ukucate "*Google takeout*", možete uraditi izvoz svojih podataka tj. eksportovati svoje podatke, kao što su: kontakti, slike, video zapisi, kalendar i još mnogo toga. Veoma korisna stvar ako ste izgubili telefon.

3. Kako zaštititi privatnost na internetu

Ovde ćemo navesti 15 praktičnih saveta kako zaštititi svoju privatnost na internetu:

1) Oni pitaju – vi ne kažete
   Samo zato što pitaju, ne znači da vi morate odgovoriti. Ako samo pravite nalog za elektronsku poštu, nema potrebe za sveobuhvatnim detaljnim profilom, a ako se pridružujete nekoj društvenoj mreži, možete ograničiti količinu ličnih podataka koje dajete na minimum. Kad Vam nije potreban odgovor na imejl od date stranice na internetu, a ipak traže vaš imejl, uvek možete izmisliti neku adresu e-pošte.
2) Kolačići
   Pazite da samo internet stranice koje posećujete smeju prikupljati informacije u obliku kolačića (tzv. *cookies*), tako što ćete podesiti svoj internet pregledač (*browser*) da odbacuje kolačiće trećih strana. Na ovaj način smanjujete mogućnost krađe podataka od strane beskrupuloznih „*tracker*"-a, na primer, putem lažnih oglasa ugrađenih u stranice koje posećujete.



Slika 5. Vizuelni prikaz trekera koji prikupljaju podatke o vama kada se poseti sajt abovetopsecret.com, Izvor:[2]

3) Lozinke
   Pobrinite se da Vaše lozinke štite Vaše podatke, a ne da služe kao pasoš prema vašim ličnim podacima. Ne koristite svuda istu lozinku i ne upotrebljavajte korisničko ime s jedne stranice kao lozinku na drugoj, jer hakeri mogu upoređivati podatke. Upotrebljavajte brojke i slova, neka velika, u kombinacijama koje nisu reči iz rečnika.
4) Vi dajete besplatno, oni to prodaju
   Istražujte malo i pogledajte profile drugih ljudi – ono što vi možete pročitati o njima, oni mogu pročitati o Vama. Objavljivanje fotografija može biti problem. Jednom kada ste svoje lične fotografije stavili na internet, imaćete vrlo malo kontrole nad njihovom upotrebom.
5) Čuvajte svoje lične podatke zaključane
   Društvene mreže su rudnik za skupljače podataka, zato im otežajte život najrigoroznijim postavkama zaštite privatnosti. U žustroj raspravi može Vam se desiti da kažete više nego što ste želeli, zato proverite šta ste objavili kako bi bili sigurni da Vam nikakvi lični podaci nisu „pobegli".
6) Zatvorite prva vrata pre nego što otvorite druga
   Ostati prijavljen na svom nalogu na društvenoj mreži ili bankarskom računu isto je što i ostaviti otključan

auto: potpuno ste otvoreni za upad hakera. Zato izbegnite rizik i odjavite se sa svojih naloga pre nego što nastavite pregledati internet.

7) Zaštitite bežičnu mrežu
   Ako koristite bežičnu mrežu, pazite da nemate uljeze. Osigurajte svoje mreže što jačom i složenijom lozinkom, kriptovanom snažnijom WPA (*Wi-Fi Protected Access*) enkripcijom, gde god je to moguće.
8) Sigurnost je dvosmerna ulica
9) Vi možda pazite na sigurnost računara i vaših podataka na internetu, no šta je sa onima koji podatke čuvaju? Izabrali ste najviši nivo sigurnosnih postavki, ali ako neka internet stranica ne može da drži vaše podatke na sigurnom, onda ste i dalje ranjivi. Dakle, proverite pouzdanost vlasnika stranica na internetu i njihovih sigurnosnih sistema.
10) Ograničavanje štete
    Razmotrite korištenje metode plaćanja koja je samo za kupovinu preko interneta. Postavite nizak kreditni limit, tako da u slučaju krađe lopov ne može napraviti veliku štetu.
11) Pazite šta potpisujete
    Ono što važi za sve, važi i za internet – pazite šta potpisujete. Na primer, neki ugovori se automatski obnavljaju i morate se u određenom trenutku izjasniti protiv produženja ako ne želite da vam se kreditna kartica tereti.
    Svaki od pretraživača *Google, Yahoo, Bing* i ostali koji nam olakšavaju svakodnevni život i poslovanje - beleže naše IP adrese i lokaciju, pa postoje neke stvari koje nikako ne treba pretraživati ukoliko vam je stalo do toga da zaštite svoju privatnost.
12) Ne pretražujte stvari koje bi Guglu mogle da otkriju vašu lokaciju AOL (*America On-Line*) je 2006. godine objavio veliki skup pretraga koje su sprovedene na njihovim stranicama, pa su tako predstavnici medija otkrili kako nije teško otkriti identitet, rodno mesto, kvart, godine, pol i druge stvari o osobi koja koristi pretraživač.
    Kolumnista Njujork Tajmsa (Dejvid Lionhard) otkrio je kako se pretraživanja razlikuju geografski. U mestima gde ljudi imaju problema sa finansijama ili zdravljem, korisnici će više pretraživati informacije vezane za zdravstvene probleme ili na primer, o prodaji proizvoda Avona.
13) Ne pretražujte informacije o zdravstvenim problemima ili lekovima.
    Tim Liber sa Univerziteta u Pensilvaniji, otkrio je kako više od 90 odsto od 80.000 stranica povezanih sa zdravljem izlaže informacije korisnika trećim stranama. Gugl prikuplja podatke sa 78 stranica koje je Liber ispitao, što oglašivačima omogućava da shvate koji korisnici imaju posebne zdravstvene probleme. Još veći problem je to što bi intimni problemi ljudi mogli da postanu dostupni onima koji žele da kupe hakovane baze podataka.
14) Ne otkrivajte pretraživačima svoje nesigurnosti.
    Pretraživanje nesigurnosti vezane za izgled osobe, kao i odnose sa drugim ljudima, mogli bi biti meta oglašivača koji jedva čekaju da prikupe takve informacije. Oni će pomoću njih pokušati da vam prodaju proizvode ili usluge.
15) Ne pretražujte ništa sumnjivo
    Kada je jedna porodica pretraživala pojmove „ranac" i „ekspres-lonac" nisu mogli ni da zamisle da će ih posetiti policija. Dogodilo se to nakon bombaškog napada na Bostonski maraton u kojem je korišćena bomba napravljena pomoću ekspres-lonca, a bila je postavljena u ranac. Žena je na internetu tražila ekspres-lonac, a suprug ranac, što je zajedno činilo sumnjivu pretragu.
    Ne pretražujte pojmove ili druge stvari koje bi se mogle povezati sa kriminalom.
16) Ne pretražujte ništa što bi Guglu moglo da pomogne
    Izbegavajte pretraživanje bilo kojih pojmova koji bi Guglu omogućili da otkrije Vaš identitet. Možete koristiti alternativni pretraživač poput *DuckDuckGo* ili probati da instalirate dodatke kao što su *AdBlock Plus, Ghostey ili Disconnect*.

Takođe bi trebalo proveriti podešavanja sigurnosti na popularnim stranicama, kao i da

se obavezno izlogujete sa društvenih mreža kada pretražujete internet.

4. Pravni aspekti privatnosti na internetu

1. Pravne pretnje

Vladine agencije koje koriste niz tehnologija dizajniranih za praćenje i prikupljanje informacija korisnika interneta su tema mnogih rasprava između advokata - zagovornika privatnosti i građanskih sloboda i onih koji veruju da su takve mere neophodne za sprovođenje zakona i održavanjem koraka sa ubrzanim promenama u komunikacionim tehnologijama.

2. Specifični primeri pravnih rasprava

Nakon odluke ministara Saveta Evropske unije u Briselu, u januaru 2009.g, Ministarstvo unutrašnjih poslova Velike Britanije usvojilo je plan da će omogućiti policiji pristup sadržaju računara pojedinaca i bez sudskog naloga. Proces, pod nazivom "daljinsko pretraživanje", dopušta jednoj strani, na udaljenoj lokaciji, da ispita sadržaj hard diska i internet saobraćaj, uključujući imejl nalog, istoriju pregledanja i pristup veb sajtovima. Policiji širom EU sada je dozvoljeno da zatraži da britanska policija sprovede daljinsku pretragu u njihovo ime. Pretres se može odobriti i sakupljeni materijal može koristiti kao dokaz na sudu, na osnovu odluke višeg oficira da je to neophodno da bi se sprečio ozbiljan zločin. Opozicioni poslanici i zagovornici građanskih sloboda su zabrinuti zbog ovog poteza, prvenstveno zbog širokog nadzora i njegovog mogućeg uticaja na ličnu privatnost. *Shami Chakrabarti*, direktor grupe za ljudska prava Liberti, kaže: "Javnost će želeti da se to kontroliše novim zakonima i sudskim nalozima. Bez tih garancija, to bi bio razarajući udarac na pojam lične privatnosti.

Magic Lantern („Magični fenjer") je softverski program FBI-a koji je bio je tema mnogih rasprava kada je objavljen u novembru, 2001. g. To je program trojanskog konja koji beleži pritiske tastera na tastaturi korisnika, čineći šifrovanje beskorisno onima koji su inficirani. [3]

5. Zaključak

U eri digitalizacije i sveopšteg eksponencijalnog razvoja internet tehnologija i informacionih sistema, prosto je nemoguće ostati van tokova i trendova. Korišćenje računara i pametnih telefona sa pristupom internetu pruža ogromne praktične mogućnosti. Savremeni život, ali i poslovanje je danas nezamislivo bez korišćenja veb sajtova, pretraživača, imejla, *cloud* servisa, društvenih mreža, jutjuba, *e-banking*- a i ostalih internet servisa i usluga.

U svemu tome postoji realna opasnost od ugrožavanja privatnosti korisnika i gubitka i/ili krađe podataka. Da bi se takvi slučajevi eliminisali ili sveli na najmanju moguću meru, potrebno je sprovesti mere zaštite, kako na strani servera i provajdera internet usluga, tako i kod korisnika pri ostavljanju poverljivih podataka na javnim računarima ili nezaštićenim bežičnim mrežama.

Zaključak ovog rada je da ne postoji potpuna privatnost na internetu, ali da postoji mogućnost da se vrsta i količina „osetljivih" privatnh informacija koje su javno dostupne na internetu svede na minimum.

Potrebno je jako pažljivo čitati sva upozorenja prilikom pristupanja aplikacijama, društvenim mrežama, komunikacionim srvisima i tačno videti čemu sve one traže pristup od vaših podataka i tek tada odlučiti da li ćete dozvoliti npr. Viber-u da ima pristup Vašem telefonskom imeniku, SMS porukama, lokaciji, kameri i mikrofonu telefona.

Dakle, ne treba s jedne strane biti ksenofobičan i odbijati sve tehničke i tehnološke novine koje dolaze sa strane, ali s druge strane treba biti pažljiv šta se i kome ostavlja od poverljivih podataka, da li su sajtovi na kojima npr. trgujemo zaštićeni *https* protokolima i preduzeti sve trenutno moguće mere opreza i predostrožnosti.

Ne postoji potpuno bezbedan i neranjiv sistem na internetu, ali mnoge krađe identiteta i podaka bi mogle da budu sprečene kada bi se i sami korisnici ponašali odgovornije.

Ukoliko ne želite da Vam neko zloupotrebi fotografiju nekada, pazite šta objavljujete na društvenim mrežama poput fejsbuka i ograničite ko može da vidi Vaše fotografije i

objave, jer čak i kada se nalog deaktivira, podaci se ne brišu, tako da nakon par godina, ukoliko se neko prijavi sa Vašim korisničkim imenom i ozinkom, svi podaci su tamo gde ste ih ostavili pre par godina.

Dakle, ukoliko damo dozvolu aplikaciji za praćenje istorije kretanja na pametnom telefonu da može da prati našu istoriju lokacija, a s druge strane na osnovu istoije pretrage na veb sajtovima moguće je napraviti naš psihološki profil (interesovanja, profesija, preferencije i slično), onda nismo daleko od Orvelove „1984." i Velikog brata koji nas sve posmatra, i fizički gde se krećemo, a i koji zna o nama dosta poverljivih i intimnih informacija.

Sve u svemu, nemoguće je ostati neprimećen na internetu i potpuno zaštititi svoju privatnost, ali se pametnim i opreznim ostavljanjem podataka, upravljanjem aplikacijama i ostalim uslugama može količina i vrsta podataka koji su dostupni o nama svesti na prihvatljivu, minimalnu meru.

Bibliografija

1. https://www.techopedia.com/definition/24954/internet-privacy avgust 2016.
2. https://en.wikipedia.org/wiki/Internet_privacy#/media/File:Screengrab_of_%27Disconnect%27,_(an_internet-browser_addon),_visualizing_the_many_trackers_on_the_website_%27abovetopsecret%27 (on_141127)-cropped.png
3. https://en.wikipedia.org/wiki/Internet_privacy
4. http://www.europarl.europa.eu/news/hr/news-room/content/20131003STO21413/html/10-savjeta-Kako-za%C5%A1tititi-privatnost-na-internetu
5. http://srbin.info/2015/09/20/sacuvajte-privatnost-ovih-pet-stvari-nikako-ne-smete-da-pretrazujete-na-Googlu/
6. http://net.hr/tehnoklik/web-social/ovaj-google-je-totalno-zlopamtilo-mislite-li-da-ste-sve-izbrisali-pretrage-gadno-se-varate/

Istorija rada:
Rad primljen: 01.10.2016.
Prva revizija: 25.10.2016.
Prihvaćen: 25.10.2016.