Vodič za paranoike: kako zaštiti osobne podatke?

Saznanje da se prati korištenje Interneta, od toga da je američka agencija za nacionalnu sigurnost NSA odobrila analizu podataka „sumnjivih“ Amerikanaca (o ne amerikancima da i ne govorimo), do Facebookovog odobravanja korištenja slika, postova i lajkova svojih korisnika za reklamiranje proizvoda svojih ulagača, čini pitanje privatnosti i zaštite osobnih podataka još važnijim.

Prema anketi Harris Interactive iz 2014 koju je provela konzultantska kuća Truste, 74 posto korisnika Interneta sada su više zabrinuti za privatnost nego što su bili prije godinu dana. Također, oko 74 posto ispitanika kažu da je manje vjerojatno da će omogućiti praćenje lokacije na webu, 83 posto je istaknulo kako je malo vjerojatno da će u buduće kliknuti na online oglase, dok se 80 posto ispitanika izjasnilo kako je manje vjerojatno da će koristiti aplikacijama kojima ne vjeruju.

Spomenuti podaci usporedivi su s prošlogodišnjim podacima. I ove godine u anketi je sudjelovalo 2000 korisnika Interneta u Sjedinjenim Američkim Državama. Najveći strahovi ispitanika odnose se na sljedeća područja:

- Online trgovina - 93%
- Online bankartsvo - 90%
- Upotreba društvenih mreža - 90%
- Upotreba mobilnih aplikacija - 85%

Časopis Computerworld zamolio je osam stručnjaka za pitanja privatnosti da preporuče kako zaštiti osobne podatke – offline i online. Neki su koraci jednostavni, no neki podrazumijevaju i vrijeme i ekspertizu kako bi se razumjeli i primijenili.

Prema Jules Polonetskyom, izvršnom direktoru Future of Privacy Forum-a, postoje tri osnovna razloga zašto ljudi žele zaštiti svoju privatnost. Prvi je skrivanje od nasilnih prodavatelja različitih proizvoda i usluga koji nerijetko prelaze granicu razumnih poslovnih odnosa. Drugi je osobna sigurnost. No, najekstremnije mjere rezervirane su za osobe koje su u strahu, jer su meta ili mogu biti meta NSA i sličnih službi.

„Potpunu privatnost je vrlo teško i skupo postići. No, razumnu privatnost koja minimizira i smanjuje naš utjecaj, odnosno ostavljanje naših otisaka online je lakše postići nego što se misli“, kazao je Rob Shavell, suosnivač i generalnih direktor u kompaniji Albine, privatnom softverskom vendoru. Dodaje kako su sve informacije o nama mogu svrstati u tri kategorije:

- podaci koje se implicitno prikupljaju - prate se naše online aktivnosti prilikom pregledavanja različitih stranica;
- podaci koji se eksplicitno prikupljaju - davanje primjerice elektroničke adrese prilikom prijave za neku online uslugu;
- javno dostupne informacije o vama (broj telefona, adresa...) koje se nalaze na Twitteru, Facebook profilu, javnim postovima, sudskim registrima i drugim evidencijama u državi.

„Prvi korak prema umanjenju online traga je da znate tko vas prati. Tu mogu pomoći *Disconnect* i *Mozilla Lightbeam*, alati koji vizualno pokazuju tko prati vaše posjete različitim web stranicama, kazao je Sid Stamm, viši menadžer za sigurnost i privatnost na Mozilli.

Pojašnjava kako je drugi korak da se shvate rizici u tome što se pokušavamo zaštiti od određene osobe. „Da li vas zabrinjava što netko prati Vaš Facebook profil? Ili da netko koga ne znate čita vaše mailove? Što više podataka želite zaštiti, čeka vas više posla.“, kazao je Sid. Dodaje kako je treći korak kontrola i da je to najteži dio. Primjerice, ako želite sakriti vaš kompletan Internet promet i svoj identitet, morat ćete koristiti Tor ili VPN cijelo vrijeme.

Kako onda minimizirati svoj trag na Internetu?

Podvucite crtu i odlučite što je privatno

Tradicionalna definicija o tome što su osobni identifikacijski podaci (OIP) - zdravstveni karton, broj kreditne kartice i sl. – stvar su prošlosti. Podaci koji prije nisu bili smatrani za OIP danas mogu biti vrlo osobni kad se sagledaju u širem kontekstu. “Komadići podataka, kada se kombiniraju, mogu reći mnogo o vama”, kaže Alex Fowler, šef za privatnost u Mozilli. Agregirani podaci, koji čine novi OIP, mogu uključivati informacije kao što vaš e-mail adresu, povijest pregledavanja i povijest pretraživanja.

Ne dijelite osobne podatke – čak i kad Vas traže

Odgovarate li na ankete putem telefona ili online? Pružate li dodatne podatke o svojim preferencijama ili možda demografske podatke prilikom prijave za neku on-line uslugu? "Većina nas informacije daje trivijalno," kaže Abine Shavell, ne shvaćajući da će sve te informacije završiti u profilima koji se mogu koristiti od strane pružatelja nekih usluga, a kasnije će se dijeliti i biti povezane s različitim agregatorima podataka.

Situacije u kojima morate ostati anonimni

Tor je krucijalan alat kada pošiljatelj kada želi poslati informacije, a istodobno ostati anoniman. Primjerice, tim se alatom koriste politički disidenti kada ne žele da se njihovo ime pojavi u prilogu informacije koje šalju," kazao je Robert Hansen, istražitelj za sigurnost i direktor za upravljanje proizvodima u WhiteHat Security vendoru. „Korištenje Tor-a košta i ponekad je gnjavaža, jer može negativno utjecati na iskustvo osoba prisutnih na webu”, ističe Casey Oppenheim, izvršni direktor u Disconnect vendoru. Tor se sastoji od open source preglednika i mreže koja radi u vaše ime s ciljem prikrivanja vašeg identiteta na način da sprečava druge od traženja mrežnog prometa povezanog s vama. "Tor na neki način usmjerava vaš promet (prokopava tunel) kroz volontersku mrežu 5.000 prijenosnika raširenih diljem svijeta. Tor štiti sadržaj u tranzitu umotavanjem slojeva enkripcije oko vaših podataka, bez mijenjanja ili dodirivanja vaših podataka u tranzitu", objasnio je Andrew Lewman.

„Vaši se podaci prebacuju iz čvora u čvor dok se ne dosegne ograničenje. U tom trenutku čvor izađe iz Tor mreže i putuje do odredišta. (Posljednji čvor koji prenosi podatke zove se izlazni čvor). Tor je u biti jako velik i distribuira se putem VPN-a te je vrlo učinkovit kada se ispravno koristi“, istaknuo je Hansen. Dodao je kako se uz pomoć Tor-a ostaje anoniman te da račun na kojeg se prijavljujete za korištenje Tor-a ne smije biti vezan uz vaš pravi identitet. Naime, posljednji čvor zna tko ste vi ako ste poslali svoje podatke u običnom tekstu i takva nesmotrenost može razbiti vašu privatnost. Hansen preporuča da se Tor koristi samo preko HTTPS-a.

Većina ljudi u Hrvatskoj vjeruje kako ne trebaju ekstremne tehnike za zaštitu svoje privatnosti. Dovoljno bi za početak bilo naučiti da ne ostavljamo bezbrižno svoje osobne podatke prilikom ponekad trivijalnih radnji na Internetu.

Radoznali mogu pročitati info i na izvoru [1].

pon, 2014-03-31 07:11 - Uredništvo**Kategorije:** Sigurnost [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1376

Links
[1] http://www.itnews.com/security/75242/paranoids-survival-guide-part-1-how-protect-your-personal-data
[2] https://sysportal.carnet.hr/taxonomy/term/30