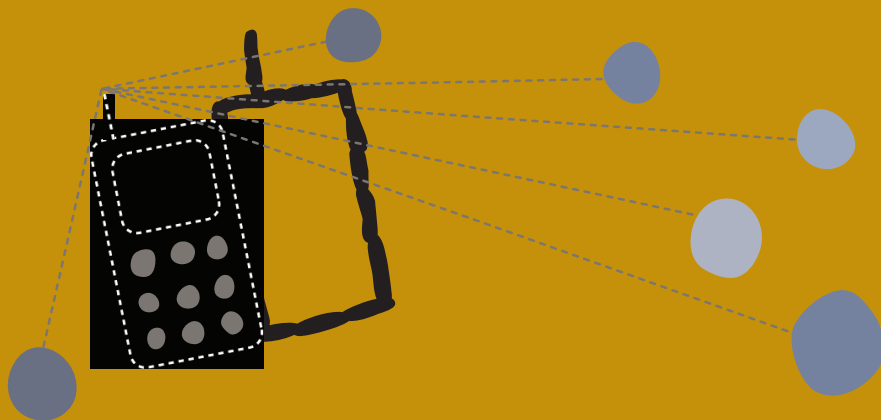


Bezbjednost i privatnost mobilnih telefona i na internetu



NOVE TEHNOLOGIJE, KAO ŠTO SU MOBILNI TELEFONI I INTERNET, MOĆNE SU ALATKE ZAGOVARANJA ALI NJIHOVO KORIŠTENJE ZA PRENOS POVJERLJIVIH INFORMACIJA NOSI I RIZIKE ZA VAS, VAŠE KONTAKTE, PRIJATELJE I KOLEGE. OVA KARTICA POMOĆI ĆE VAM DA INFORMACIJAMA PRISTUPITE NA SIGURAN NAČIN I DA ZAŠTITITE VAŠE PODATKE KADA KORISTITE MOBILNE TELEFONE I INTERNET.

ŠTA JE DIGITALNA SIGURNOST I PRIVATNOST?

Znači da su informatička prava i digitalna sigurnost kompromitovani uključuju:

- Misteriozna promjena lozinki
- Privatne poruke koje je očito pročitao neko drugi osim osobe kojoj su namijenjene
- Websajti koji su postali nedostupni iz određenih država
- Vladini zvaničnici iznose podatke o privatnoj korespondenciji, uključujući datume, imena ili teme o kojima je razgovarano
- Razgovori mobilnim telefonom za koje ljudi smatraju da su praćeni

DA LI BI ME TO TREBALO BRINUTI?

Ako će takav scenario kompromitirati vaše projekte ili izložiti vas ili vaše kontakte progonu, onda bi trebali biti zabrinuti. Znanje i softverska rješenja potrebna za takve napade na vašu digitalnu privatnost često su dostupni na internetu. Ako napadač posjeduje dostatan pristup internetskoj ili infrastrukturi mobilne telefonije u vašoj zemlji, potrebna tehnologija je relativno jednostavna. Vladine agencije, provajderi internet usluga (ISP) i mobilni operateri uživaju privilegirani pristup toj infrastrukturi, ali kolege

iz kancelarije, susjedi i operateri internet kafea takođe mogu imati određeni pristup.

KOJA SIGURNOSNA PITANJA POKRIVA OVA KARTICA?

Ova kartica fokusirana je na mobilne telefone i alatke na internetu. Ipak, postoje brojne druge tehnologije koje vas mogu napraviti ranjivim na cenzuru, nadzor i progon. Mada o njima u ovoj prilici ne raspravljamo, redovno ažuriranje operativnog sistema koji koristite na računaru, pouzdan anti-malware softver i konzistentne procedure čuvanja materijala su najznačajnije osnovne mjere opreza koje možete poduzeti. Ako postoji razlog zbog kojeg sumnjate da su vaši računari i uređaji za čuvanje podataka, uključujući i back-up uređaje, u opasnosti od gubljenja, krađe ili zaplijene, ili da je vaša organizacija podvrgnuta ciljanom nadzoru putem interneta (ili ako je to stalna pojava u regionima u kojima radite), onda bi trebalo da pogledate Tactical Techov Sigurnosni komplet.

Alatke zagovaranja na internetu

Kada koristite alatke na internetu, kao što su Blogger, Facebook i twitter, za potrebe mobilizacije ili koordinacije, upamtite da informacije koje čuvate na takvim platformama postaju, u određenom stupnju, vlasništvo operatera, i da mnoge takve alatke izlažu puno više informacija nego što možda mislite.

Kada povjeravate osjetljive podatke operateru neke online alatke, dobro pročitajte njihovu politiku privatnosti ili ponuđeni korisnički ugovor. Upamtite da čak i najprosvjetljenija politika ostavlja vaše informacije pod direktnom kontrolu administratora platforme, koji onda može podijeliti, prodati ili postaviti te informacije na pogrešno mjesto bez vašeg znanja i dozvole. Čak i kada ukinete svoj korisnički nalog, mnogi takvi sajтови zapravo i ne pobrišu sadržaje koje ste postavili ili vaše lične podatke. Konačno, osim ako korištenje datog komercijalnog servisa nije bitno ili neophodno, iz razloga dostupnosti ili povezivanja sa korisnicima nižeg profila, razmislite o korištenju alternativa koja su puno naprednije po pitanju prava: Blip.tv umjesto YouTubea; riseup.net umjesto Gmaila. Ako posjedujete tehničke resurse, možete voditi i vlastite internet usluge.

Ako koristite komercijalne platforme, poduzmite mjere opreza kako bi se zaštitili od zlonamjernih osoba koje znaju kako iskopati privatne informacije na takvim servisima. To se naročito odnosi na platforme društvenih mreža kao što su Facebook i MySpace. Usvojte detaljno razumijevanje opcija privatnosti koje su ugrađene u te platforme i razmislite od vrstama informacija koje možete nenamjerno otkriti o sebi li o vašoj organizaciji; na primjer, vaše pravo ime, gdje živite, gdje ste putovali ili informacije o planiranim događajima i sastancima. Posmatrane tokom dužeg perioda, te informacije mogu dati pregled vaših životnih i radnih navika.

Jedna korisna tehnika je kreiranje više naloga na internet servisu koji koristite, što će vam omogućiti da koristite različite naloge ili profile za različite projekte, i da održavate testne naloge koje možete koristiti da „špijunirate“ sami sebe. Vaša privatnost će biti bolje zaštićena ako možete da provjeravate, na različite načine, šta je prikazano o vašem korisničkom nalogu; na primjer, pretraživanjem interneta ili ljudi koji posjeduju privilegirani pristup.

LOZINKE

Većina resursa na internetu oslanja se na samo jednoj lozinci u zaštiti vašeg profila. Ako zlonamjerna osoba ili organizacija sazna tu lozinku, nije ni važno da li imate povjerenja u administratore sajta, ili kako ste pažljivo testirali vašu privatnost: odmah ćete izgubiti tajnost i anonimnost vaših podataka.

Manje znani načini probijanja neke lozinke: Neko može instalirati malware na računar koji koristite kako bi se logirao na sigurni websajt. Ili, neko može nadzirati vašu internet vezu kada se logirate na nesiguran websajt.

Kako bi se zaštitili od prve vrste napada, koristite vlastiti računar ili računar koji održava osoba kojoj vjerujete, i osigurajte se da je operativni sistem i anti-malware softver redovno ažuriran na najnoviju verziju. Kako bi se zaštitili od druge vrste napada, najpopularniji servisi za email, društveno umrežavanje, blogiranje, mapiranje i video platforme na internetu nude sigurne konekcije - HTTPS. Možete provjeriti da li je vaša konekcija na webstranici sigurna ako u liniji za adresu u pretraživaču stoji 'https://' (umjesto samo 'http://'). Sa druge strane, mnoge internet alatke ne koriste

HTTPS za zaštitu informacija koje podnosite ili kojima pristupate na njihovim sajtovima, osim vaše lozinke. Kao rezultat, ako neko prati vašu vezu dovoljno dugo, saznaće šta čuvate na određenom sajtu. Najbolja zaštita u toj situaciji je da tražite internet alatke koje koriste HTTPS na svim stranama.

ZAOBILAŽENJE CENZURE

Možete koristiti sigurne internet proksije, alatke za zaobilaženje cenzure ili softver za osiguravanje anonimnosti, na primjer Tor, da prikrivate vaš identitet na websajtima koje koristite ili kako bi zaobišli internet filtere. Te alatke su korisne kada želite da pristupite blokiranim sajtovima; na primjer, za potrebe istraživanja, ili da podnesete ažurirane podatke na internet platforme kao što je Facebook.

BITI ANONIMAN/NA NA INTERNETU

Softver za osiguravanje anonimnosti kakav je Tor koristan je kada ne želite da otkrijete koje ste websajtove posjetili. Tor prebacuje vašu konekciju između nekoliko nasumično odabranih volonterskih računara kako bi spriječio da čak i vaš internet provajder ili ovlašteni vladini službenici saznaju što ste radili na internetu. Ipak, nemojte koristiti Tor za slanje informacija na nesigurne websajtove ili primanje informacija sa njih. Ako ste povezani na websajtu koji podržava HTTPS, moguće je da će neki od računara koji vam dobrovoljno omogućava korištenje Tor-a prati sadržaj dok se postavlja. Tor je veoma siguran softver, ali dok ga koristite znatno usporava vašu internet konekciju.

Mobilni telefoni

Zagovarači širom svijeta koriste mobilne telefone, ali često se dešava da na njima čuvaju privatne informacije. Osim lista kontakata, mobilni telefon može sadržavati i istoriju poziva, kalendare, tekstualne poruke i emailove.

Razmislite o informacijama koje čuvate u telefonu, imajući u vidu naročito činjenicu da se mobilni telefoni često konfiskuju. Na primjer, vjerovatno ne morate čuvati sve vaše kontakte u mobilnom telefonu ako vaš rad uključuje osjetljive informacije o pravima, i trebali bi izbrisati informacije sa mobilnog telefona i sa SIM kartice uvijek kada možete. Prilikom organiziranja događaja ili mobilizacije mreža, jedna dobra ideja je korištenje anonimnih, pre-paid SIM kartica i povremena promjena aparata. Imajući u vidu kako je lako pretraživati i filtrirati SMS, poželjno je izbjegavati osjetljive ključne riječi kod slanja tekstualnih poruka. Kada su uključeni, mobilni telefoni mogu biti iskorišteni da odrede vašu tačnu lokaciju. Učesnici poverljivog skupa trebalo bi da isključe telefone i izvade baterije prije nego što izađu, i da sačekaju povratak kući pre nego što ponove ubace baterije i uključe telefone. Provajderi usluga mobilne telefonije imaju pristup podacima o svim pozivima: Koga ste zvali, kada i gdje ste bili kada ste zvali. Provajderi mogu biti zakonom obavezani da čuvaju ili predaju te podatke na zahtjev vlasti, i mogu čuvati te podatke nekoliko godina.

AKTIVNOST: IDENTIFIKACIJA SIGURNOSNIH RIZIKA

Iskoristite sljedeća pitanja kako bi ste ocijenili sigurnosne rizike sa kojima se suočavate i odlučili koje alatke možete koristiti za odstranjivanje tih rizika.

1. **Radim sa osjetljivim informacijama.** Ono što je bitno znati jeste da li radite sa osjetljivim informacijama koje bi možda mogle da natjeraju nekoga da poželi pratiti vaš rad. Da li ste uključeni u aktivnosti koje vlasti, policija, vojska ili neka privatna kompanija mogu smatrati osjetljivima ili remetilačkima? Ako je odgovor da, neprimjenjivanjem nekih sigurnosnih mjera možete sebe i druge dovesti u opasnost.
2. **Radim sa ljudima čiji identitet i lični podaci moraju ostati tajni.** Možda sakupljate privatne informacije od ljudi kojima pružate podršku, kao što su informacije o nasilju u porodici, prisilnom radu ili silovanjima.

Ako vam ljudi dostavljaju informacije koje ih mogu dovesti u opasnost, morate poduzete mjere kako bi osigurali da će te informacije ostati tajne.

3. **Ponekad komuniciram internetom sa ljudima koji rade sa povjerljivim informacijama.** Čak i kada smatrate da se lično ne suočavate sa sigurnosnim rizicima, ako komunicirate na internetu sa osobama koji se sa takvim rizicima suočavaju, možete postati cilj ljudima koji se protive njihovom radu. Oni mogu iskoristiti vas kako bi došli do privatnih informacija o drugim ljudima.
4. **Imam pristup ili postavljam sadržaje, koji se mogu smatrati osjetljivima, na internetu.** Možda postavljate informacije na websajtove posvećene ljudskim pravima, ili postavljate članke u kojima se suprotstavljate grupama za koje vjerujete da ne poštuju ljudska prava. Čak i obična posjeta osjetljivih sajtova na internetu može od vas napraviti cilj praćenja.

Resursi o sigurnosti i privatnosti na internetu

Za više informacija i za snimanje sigurnosnih alati, pogledajte:

1. **„Security in a box“ (Sigurnosni komplet)** pripremili su Tactical Tech i Front Line kako bi odgovorili potrebama za sigurnošću i privatnošću zagovarača i branitelja ljudskih prava. <http://securitz.ngoinabox.org/>
2. **Digitalna sigurnost i privatnost za branitelje ljudskih prava, koju je proizveo Front Line,** daje korisne informacije o procjeni i rješavanju digitalnih prijetnji. <http://bit.ly/1aCkSs> (frontlinedefenders.org)
3. **Mobiles in-a-box (Mobilni komplet),** proizveden od strane Tactical Tech-a, posvetio je čitavo jedno poglavlje privatnosti i sigurnosti kod mobilne telefonije. <http://mobiles.tacticaltech.org/security>
4. **Anonimno blogiranje sa Wordpress-om i Tor-om.** Global Voices kreirao je ovaj vodič kao podršku zagovaračima ljudskih prava koji žele da otkriju istinu i izraze se preko interneta, ali koji se time mogu izložiti rizicima. <http://advocacy.globalvoicesonline.org/projects/guide/>
5. **Budite anonimni na internetu i izbjegnite cenzuru.** Tor je dizajniran sa ciljem pojačane anonimnosti vaših aktivnosti na internetu, a može poslužiti i za zaobilazanje filtriranja na internetu. Možete ga snimiti u vaš računar ili pokrenuti ga sa USB memorije. <http://www.torproject.org/>