**Problem zaštite na internetu**

**Etika javnog komuniciranja**

[www.maturski.org](http://www.maturski.org/)

**Privatnost u 21. veku. Da li ona uopste postoji?**

Kao sto je poznato problem zastite privatnosti nije samo vezan za internet niti je sa internetom poceo. Koren problema javlja se jos ranije I razvijao se od prvih fotoaparata I kamera do “tagovanja” na “fejsbuku”. Sada kada pisem ovaj tekst, tesko mi je uopste da razmisljam o privatnosti I da je na pravi nacin definisem. Gore napisano pitanje je sve sto mi stoji u glavi. Kako privatnost danas moze da postoji kada “fejsbuk” zna sve sta sam radila u proteklih dve godine koliko sam clan.

Kako bih se sto bolje pripremila za pisanje ovog teksta pregledala sam svoj profil na “fejsbuku” I trudila se da ga gledam “tudjim” ocima, ocima ljudi koji su mi prijatelji na tom sajtu I koji imaju pristup mojim podacima. Shvatila sam da je veliki deo mog zivota tu predstavljen kao otvorena knjiga, dostupna svima za citanje I “izvlacenje” informacija.

Kad bi neko hteo to da uradi, mogao bi da tacno utvrdi sta sam radila u proteklih nekoliko meseci I to tako precizno da, ne samo da bi znao sta sam radila kog dana, nego cesto i u koliko sati i gde.

Cudno je razmisljati o tome i pomalo zastrasujuce. Ljudi koji su mi sada prijatelji mozda to nece biti i u buducnosti a i dalje ce imati pristup takvim informacijama.

**No, da se vratimo na pocetak.**

Svako vreme nosi sa sobom neke promene, a 21. vek sa sobom doneo je nesto sto je pomerilo granice. Nove tehnologije, najsladji plod 21. veka sa sobom je donelo mnogo toga sto nam je olaksalo zivot i rad. Dobili smo na informisanosti, mobilnosti, vremenu i svemu onome sto su novi izazovi savremenog poslovanja i nacina zivota ugrozavali. Nove tehnologije doprinele su da se zivi brze i da ja mogu ovaj rad koji sada pisem profesoru da posaljem na email adresu, dok bih za to nekada utrosila mnogo vise vremena u odlasku do fakulteta i nazad.

**A onda je dosao Facebook**

Zivot je takav, sastoji se od raznih trenutaka koje ostavljamo iza nas, raznih ljudi i prica koji postaju delovi nase proslosti i u buducnosti zive kroz nase secanje.

Facebook je na neki nacin pobedio vreme i prostor. On je na jednom mestu okupio sve, izazvavsi toliko puta onaj cuveni “wow” efekat kada nas pronadje neko koga nismo videli toliko dugo. I ta cinjenica da je Facebook postao centralno mesto za komunikaciju sa nasim prijateljima, bili oni iz kuce pored nas ili sa drugog kraja planete, je razlog njegove super-popularnosti i broja od preko 500 miliona korisika.

**Kako nas pre nisu ovako povezali mobilni telefoni ili email?**

U nekoj meri jesu ali zahtevali su dodatnu aktivnost koja obicno nedostaje – trazenje broja telefona ili pamcenje email adrese koje nije uvek tako lako kao pamcenje imena druga iz klupe, koje je na Facebook-u dovoljno da do njega i dodjemo.

Procitala sam negde poredjenje koje mi se mnogo svidelo i koje kaze da su drustvene mreze ustvari dnevnik koji nikada nismo voleli da pisemo. I to jeste istina. Nase aktivnosti i aktivnosti nasih prijatelja ostaju iza nas zabelezene, samo sto umesto slova na papiru imamo fotografije, snimke, statuse, komentare.

Gledajuci nase slike na “fejsbuku” ili statuse, mozemo se tacno setiti sta smo u odredjenom periodu naseg zivota radili, kako smo razmisljali, gde smo gresili i generalno – kakve smo osobe bili. Ovo je ono sto nas vezuje za ovaj sajt i zato za njega, za razliku od mnogih drugih, mozemo da kazemo da ga “volimo” i da smo od njega “zavisni”.

**Facebook se koristi i u poslovne svrhe**

Veliki broj korisnika koje okupljaju drustvene mreze doveo je do toga da i kompanije pocnu ozbiljnije da bave njima. Njihova nainteresantnije mogucnost jeste precizno ciljanje odredjenih ciljnih grupa, cime su marketari napravili korak dalje kada je marketing “1 na 1” u pitanju. Gomila informacija koje odajemo o nama samima, poput godista, lokacije ili licnih interesovanja predstavljaju neverovatno vredne podatke kada je u pitanju plasiranje kampanja, čime se znatno smanjuju troškovi marketinga.

Svoj pun potencijal na društvenim mrežama doživljava i marketing “od usta do usta”. Kao prvenstveno servis za komunikaciju, aktivnosti koje se dešavaju oko određenog brenda mogu u mnogome doprineti poslovanju određene kompanije, kako su prijatelji oni od kojih ćemo najradije primiti savet kada je odlučivanje za određeni proizvod/uslugu u pitanju.

**Gde nastaje problem?**

Sve to što delimo sa prijateljima retko kada ostaje „između nas“, gotovo uvek te sadržaje - fotografije, linkove, statuse i postove mogu videti i neki ljudi sa kojima nismo želeli da ih podelimo. A to na netu ostaje i sutra i prekosutra.

Možete da odbijete da koristite internet i da ne gradite svoj digitalni identitet. Ipak, i ako se vi ne bavite internetom, on se već bavi vama. I ako vas zvanično nema na “fejsu”, verovatno je neko od vaših prijatelja postavio fotografiju na kojoj ste i vi. Verovatno vas negde i pominju. A možda pominju nekog ko se zove isto kao vi, a nije baš osoba sa kojom biste želeli da vas pomešaju.

Danas se kaže – Ako te nema na “netu”, ne postojiš. To što nemamo izgrađen digitalni identitet može značiti da smo informatički i informaciono nepismeni. Ili da jednostavno nismo prepoznali kakve prednosti nudi internet.

Bolje da mi vodimo priču o sebi i kontrolišemo šta se o nama priča. Cilj nam je da upravljamo svojim digitalnim identitetom tako da se o nama vidi samo ono što mi želimo da se vidi, a da ublažimo sve što nam se možda ne dopada. Pažljivom izgradnjom pozitivnog onlajn identiteta i imidža možete mnogo da doprinesete izgradnji vašeg kredibiliteta u privatnom i poslovnom životu.

**Ugrožavanje privatnosti**

O prednostima društvenih medija smo dovoljno čuli ali uvek treba sagledati i onu drugu stranu medalje. U ovom slučaju to je ugrožavanje privatnosti pojedinaca, koji nesebično deleći informacije mogu dovesti sebe u opasnost. Glavni problem je u tome što smo mi ti koji emitujemo informacije a podešavanja o privatnosti, iako napredna, uglavnom predstavljaju deo o kom se ne brinemo previše i ako bi trebalo. Od krađa identiteta i ličnih podataka, pa dovođenja u opasnosti otkrivanjem svoje fizičke lokacije, privatnost je postala broj jedan tema kada su protivnici društvenih medija u pitanju.

Sa druge strane često ćete čuti i negativne komentare o odavanju naših privatnih podataka u marketinške svrhe. Marketing “1 na 1” zvuči kao san svakog marketara, ali ujedno se može i tretirati kao manipulacija krajnjih korisnika. Nažalost, ovo nije problem samo društvenih mreža, već i interneta generalno, a koliko će daleko sve ići ostaje da vidimo.

Nedovoljan broj njih brine o svojoj bezbednosti, sigurnosti i privatnosti u okviru ove mreže. Ranija verzija “Fejsbuka” štitila je maloletne tako što su im profili bili vidljivi samo prijateljima. Više nije tako. Čak i ako ne mislimo na najcrnje opcije, poput kriminalnih radnji čija žrtva moze bilo ko da postane, treba misliti o opcijama privatnosti.

Neki ljudi, na primer ne dozvoljavaju drugima da vide čak ni kompletan spisak njihovih prijatelja. Drugi, s druge strane, ne kriju i ne zatvaraju ništa. Kada o ovome govorimo, to svakako nije pitanje ukusa.

**Internet i vi – drugari ili neprijatelji**

Zavisno od toga koliko ste pažljivi, možete samo da delimično ublažite štetu i sačuvate barem deo svojih privatnih podataka od tuđih očiju. Otvorite web browser. Upišite neku reč u pretraživač. Otvorite neku web stranicu. Svaka od tih radnji, verovali ili ne, odaje neke informacije o vama, iako vas niko nije pitao za ime i prezime.

Stvari postaju još gore kad se ulogujete na neki internet servis, kao što je Facebook ili MySpace. Samim tim činom pristajete na prilično dug spisak informacija koje ti servisi mogu da sakupe od vas i koriste u svrhe oglašavanja, internih statistika ili nečeg sasvim drugog. Ako niste preduzeli određene korake da sačuvate svoju privatnost, kompanije kao što je to, na primer, Google znaju ko ste, odakle se konektujete na Internet, koje stranice volite da posećujete, koji su vaši društveni kontakti, šta kupujete na Internetu i slično. Ovde odmah treba ukazati na ono loše - nema načina, osim ako ne preduzmete neke ekstremne mere, da sasvim sačuvate svoju privatnost na Internetu. Ipak, možete bar da umanjite količinu privatnih podataka koje rasipate dok ste na Internetu.

Kao prvo, većina web stranica koje posećujete može na vašem računaru da ostavi cookie, malu datoteku pomoću koje može da prati koliko često posećujete određenu stranicu ili kuda ste s nje otišli. Podršku za cookie možete ugasiti u svakom web browser-u, ali vam onda pola internet stranica neće raditi. Dakle, tu ne možete da učinite puno, osim da izbegavate pojedine stranice koje su poznate po agresivnoj upotrebi cookie-ja. Nešto slično važi i za web pretraživače, koji mogu da pratiti vašu IP adresu (niz od maksimalno 12 brojeva koji jednoznačno identifikuje vaš računar na Internetu), vreme pretraživanja, ključne reči koje ste koristili i tome slično.

Stvari postaju ozbiljnije kada počnete aktivnije da unosite podatke o sebi. Primera radi, društvena mreža Facebook zahteva od korisnika da napišu svoje pravo ime i prezime. Slike, poruke i ostale podatke koje ostavljate na društvenim mrežama i drugim servisima često je moguće pronaći običnim pretraživanjem Google-a. Čak ni vaša e-pošta nije sigurna. U određenim slučajevima internet provajder će možda dati vaše podatke nekom organu vlasti (naravno, ovo zavisi od toga u kojoj državi se nalazite vi i servis e-pošte koji koristite).

Slično važi i za razne druge podatke za koje možda smatrate da su privatni; na primer, prilikom otvaranja internet domena, od vas će se tražiti vaši pravi podaci, uključujući ime, prezime i adresu, koji će (ako posebno ne zatražite i ne platite privatnost) biti potpuno javni i dostupni svima na raznim whois servisima. Na kraju, tu je i najozbiljnija pretnja po vašu privatnost, a to su razni virusi i drugi zlonamerni programi koji mogu da ukradu vaše šifre, brojeve kreditnih kartica i druge osetljive informacije i da ih pošalju na udaljenu adresu.

Postavlja se pitanje kako se onda zaštiti. Ljudi ostavljaju svoje licne podatke, cak I ako to nije apsolitno potrebno. Veliki problem se javlja kada korisnici, ne svesni rizika, ostavljaju na svim mestima koje posecuju na internetu istu sifru.

Kao prvo, treba da izbegavati ostavljanje svojih ličnih podataka ako to nije apsolutno potrebno. Ako negde i ostavlimo lične podatke, uvek koristite lozinku različitu od one koju koristitimo na manje važnim web servisima, Koristite antivirusne programe i najnovije verzije web browser-a (preporuka je Firefox, ali novije verzije svih web browser-a imaju pristojnu zaštitu od zlonamernih internet stranica), i izbegavajte sumnjive internet stranice, pogotovo one koje nude besplatni softver ili materijal za odrasle. Korišćenje firewall-a i anti-spyware softvera takođe je preporučljivo.

Ako baš morate da se registrujete na nekom sumnjivom servisu, ili na nekom koji vam nije od posebne važnosti, koristite jednokratne e-mail adrese koje služe samo za registraciju i koje će vas zaštititi od spama. Jedan takav servis je Mailinator. Na društvenim mrežama i ostalim servisima za razmenu poruka, slika ili drugih podataka nikad ne ostavljajte podatke za koje ne želite da ih neko drugi vidi. Primera radi, ako postavite neku sliku na Facebook, taj servis ima pravo da je koristi u svoje svrhe, a da vas ni za šta naknadno ne pita. Srećom, danas velike kompanije kao što su Google i Facebook moraju da paze na privatnost korisnika, pa se treba dobro upoznati s takvim servisima i videti koje su vam mogućnosti na raspolaganju. Dobar primer je Facebook, koji vam omogućuje izuzetno detaljno podešavanje sigurnosnih opcija, kao i onih povezanih s privatnošću. Korisnici ih često zanemaruju, pa ostavljaju svoj profil otvoren, možda i ne znajući da svaki od 160 miliona korisnika Facebook-a može da vidi njihove podatke.

Treba imati na umu da ako se i, raznim opcijama koje postoje unutar samog “Fejsbuka”, zastitimo od drugih korisnika nismo se zastitili od samog “Fejsbuka”. Kada pazljivo procitate uslove koriscenja shvaticete da je jedini nacin da se potpuno zastitite zapravo da ne koristitite “Fejsbuk” a to vazi i za sve druge onlajn servise. Takodje, mnogi takvi servisi dozvoljavaju promenu podesavanja vezanih za privatnost, a ta podesavanja nisu sama po sebi naklonjena nama, zato svaku onlajn aplikaciju koju koristimo (na primer Gmail, MySpace, Flickr) dobro treba da pogledamo koje opcije vezane za privatnost mozemo da promenimo u podesavanjima.

**Za kraj 5 najčešćih propusta u Email bezbednosti**

1. Korišćenje samo jednog email računa

Dobar savet je da, kao email korisnici, imate minimum tri email računa. Vaš poslovni račun bi trebalo da bude korišćen isključivo za razgovore koji se odnose na vaš posao. Drugi email račun bi trebalo da bude korišćen za lične razgovore i kontakte, i vaš treći email račun kao opšti za sve rizične emailove koje dobijate. To znači da bi uvek trebalo da se prijavljujete na newslettere samo putem trećeg email računa. Istovremeno, ako morate da postavite vaš email račun online, kao npr. za lični blog, trebalo bi da koristite samo treći email račun.

Dok se vaši prvi i drugi email računi mogu plaćati ili biti besplatni, vaš treći račun treba uvek da bude besplatan, kao npr. Gmail ili Yahoo. Trebalo bi da imate u planu i promenu ovog računa svakih šestmeseci, kako ovaj email račun ne bi eventualnopostao spamovan kada rukovalac newslettera odlu-či da proda vaše ime ili ako spamer ukrade vašu email adresu na web sajtu.

1. Zaboravljanje telefona kao moguće opcije

Jedna od najznačajnijih lekcija email bezbednosti je da bez obzira na to koliko koraka preduzimate daosigurate vaš email, nikada nećete biti potpunoosigurani, naročito ako koristite javni kompjuter. Paukoliko ne morate da šaljete snimke ili da komunicirate širom Zemlje, radije razmislite o upotrebijednostavnog telefonskog razgovora nego o opcijiupotrebe emaila. Dok telefonski razgovor možepotrajati nekoliko dodatnih minuta, u poređenju sadostupnošću emaila putem javnog kompjutera, telefonski poziv je daleko sigurnija opcija i ne ostavlja pisani trag.

1. Korišćenje nesigurnih email računa za slanje iprimanje osetljivih korporativnih informacija

Velike korporacije ulažu velike sume novca kako bibili sigurni da su njihova kompjuterska mreža iemailovi bezbedni. Uprkos njihovim naporima, neobazrivi zaposleni upotrebom ličnih email računamogu svojim ponašanjem ugroziti poslove kompanije. Zato se obezbedite kako ne biste rizikovalisigurnost kompanije i vašeg posla, prenošenjemosetljivih podataka kompanije putem vašeg ličnogkompjutera ili email adrese.

1. Zaboravljanje brisanja skrivene memorije, istorije i lozinka browsera

Nakon upotrebe javnog terminala, važno je da zapamtite da izbrišete skrivenu memoriju, istoriju i lozinke na browseru. Mnogi browseri automatski čuvaju tragove svih web stranica koje ste posetili, a neki pojedinih lozinki i lič-nih informacija koje ste uneli na nalogu, kako bi vam pomogli da ispunite slične forme ubuduće. Ako ove informacije dospeju u pogrešneruke one mogu biti ukradene. Važno je da internet korisnici budu svesni da brisanjemskrivene memorije browsera na javnim kompjuterima mogu obrisati i privatne informacijepre nego što ih hakeri preuzmu.

1. Nezatvaranje browsera nakon odjave

Kada se proverava email u biblioteci ili internet kafeu često se dešava da se korisnik samo odjavi sa email računa kada završi sa radom. Morate biti sigurni da ste kompletno zatvorili ibrowser. Razlog za to je što pojedini emailservisi pokazuju vaše korisničko ime (ali ne ivašu lozinku) čak i nakon što ste se odjavili.

**Log out**

Nove tehnologije donele su promene. Promenile su nacin zivota i rada i na neki nacin poimanja stvarnosti. Nasi zivoti sada su “onlajn”, mi tamo zivimo, tamo nam je druga kuca, tamo su nam prijatelji, tamo imamo posao i ubijamo dosadu. Ali tamo su i problemi.

Nove tehnologije dale su nam mogucnost da se edukujemo, da podelimo sa drugima svoja licna iskustva, pogledamo fotografije nama nepristupacnih mesta, da znamo sve o svakome a da ujedno ne znamo nista.

I to sve radimo nevino, ne razmisljajuci o posledicama, prepustamo se toj reci koja nas nosi ponekad i do mracnih dubina prevare i kriminala. Tu reku mi ne znamo da obuzdamo i pitanje je da li se moze obuzdati. Mi joj se samo prepustamo, u njoj uzivamo, komentarisemo fotografije svojih drugara i sa njima, i mnogim drugim nepoznatim ljudima, delimo nasu privatnost. Privatnost koja sve manje postaje “privatna” i nasa.

[www.maturski.org](http://www.maturski.org/)