Privatnost na mreži – izvor nastavnog sadržaja

* Svaki put kada pristupamo internetu, služimo se društvenim mrežama, plaćamo online, čitamo novosti na portalima, objavljujemo slike ili sudjelujemo u raspravi, ostavljamo digitalne „mrvice“ koje sadrže informacije o nama, našim akcijama i djelovanju na internetu.
* Nakon što sve te informacije skupimo zajedno dobivamo profil koji ocrtava naše ponašanje na internetu.
* **Digitalni trag**, otisak ili sjenu čini jedinstven skup digitalnih aktivnosti, akcija, doprinosa te komunikacije putem interneta i digitalnih uređaja kojoj se može ući u trag.

Pasivni digitalni tragovi

* Oni tragovi koje ostavljamo bez znanja ili namjere. Na primjer, stranice broje koliko često ih posjećujemo, a ti se podaci prikupljaju pasivno jer im mi kao korisnici ne dajemo dopuštenje da te podatke prikupljaju. Riječ je o skrivenom procesu za kojeg ne znamo da se događa i odvija se u pozadini, a o njemu nismo obaviješteni.

Aktivni digitalni tragovi

* Uključuju sve one informacije koje smo ostavili na internetu svjesno i namjerno kao što su objave na društvenim mrežama ili komentari ispod nekog video zapisa ili novosti na nekom portalu.
* P**rijave na liste elektroničke pošte (engl. mailing lists)**
* **Kolačići koje prihvaćamo** prilikom služenja pojedinim internetskim stranicama.

Savjeti za ostavljanje pozitivnog digitalnog traga

Istražite svoje digitalne tragove

* Razmišljajte prilikom objavljivanja
* Prilagodite svoje postavke privatnosti
* Vladajte svojim korisničkim računima
* Koristite više adresa elektroničke pošte
* Koristite online servise za zaštitu podataka
* Izgradite svoj ugled ponašanjem
* Imate pravo na zaborav.

Zahtjev za uklanjanje digitalnih tragova

* Sud Europske unije donio je odluku o pravu osobe da bude zaboravljena na mreži, odnosno pravu na uklanjanje digitalnih tragova.
* Ako ste naišli na rezultat pretraživanja na web tražilici za kojeg ne biste htjeli da bude dostupan (a koji vodi do sadržaja koji je objavljen unutar granica članica EU), možete podnijeti zahtjev za njegovim uklanjanjem putem njihove usluge EU Privacy Removal.

Osobni podaci

Osobni podaci su svi podaci koji se odnose na pojedinca čiji je identitet utvrđen ili se može utvrditi, odnosno definiraju svakog pojedinca kao jedinstvenu osobu.

* Osobni su podaci sljedeći:**ime, prezime, datum i mjesto rođenja, OIB, broj telefona, kućna adresa, *e-mail* adresa, osobna fotografija, broj osobne iskaznice, podaci o obrazovanju i stručnoj spremi, biometrijski podaci**(otisak prsta, snimka šarenice oka), **financijski podaci**(plaća, računi u banci...), **podaci o lokaciji**(na mobilnom uređaju).
Osobni podaci druge osobe najčešće se koriste za sklapanje lažnih ugovora, krađe identiteta, otvaranje lažnih profila i sl.

Kako zaštititi osobne podatke?

* Vodite računa o tome kome i zašto dajete osobne podatke
* Ne odgovarajte na poruke u kojima se traži upisivanje vaših podataka
* Ne bacajte u koš dokumente na kojima su vaši podaci (ili bilo čiji podaci)
* Zaštitite svoje profile jakim lozinkama
* Dvostruka provjera autentičnosti (na računima elektroničke pošte, posebno na društvenim mrežama).

Što učiniti ako dođe do zlouporabe?

Prijaviti na stranicama Agencije za zaštitu osobnih podataka

Jake lozinke

* Jaku lozinku kreirajte kombinacijom više znakova uključujući specijalne znakove.
* Kako bi lozinka štitila vaš korisnički račun, treba zadovoljavati sigurnosne kriterije: mora imati barem 6 znakova, jedno veliko slovo, jedno malo slovo i jedan broj .
* Što više znakova postavite u lozinku, teže ju je otkriti.
* Kod kreiranja lozinke treba izbjegavati korištenje podataka koji se lako povezuju s Vama (ime, prezime, datum rođenja i sl.)

Kolačići

* Želimo kupiti karte za koncert pomoću interneta. Unosimo tražene podatke, ali slučajno zatvorimo stranicu. Pri ponovnom otvaranju stranice, naši su podaci ostali popunjeni. Kako? Za to su zaslužni **kolačići**koji su pratili naš unos.
* Kolačići sami po sebi nisu opasni, ali mogu poslužiti tvrtkama za reklamiranje proizvoda.
* Postoje i opasni kolačići koji služe za praćenje (engl.*tracking cookies*), a koriste se tako da pamte zapise o korisnikovoj povijesti surfanja koja može uključivati i osobne podatke. Zatim se šalju autoru kolačića na obradu.
* Kolačići mogu biti iskorišteni za narušavanje privatnosti korisnika, a zbog mogućnosti zloupotrebe je u Europskome parlamentu i Vijeću Europske unije 2002. donesena Direktiva o privatnosti i elektroničkim komunikacijama. Ta Direktiva omogućava korisniku da sam odluči želi li prihvatiti ili odbiti kolačiće.
* U Republici Hrvatskoj je ova mjera od 2011. godine dio Zakona o elektroničkim komunikacijama.
* Važno da prilikom odobravanja obavijesti o kolačićima na internetskim stranicama budemo svjesni što i zašto odobravamo.

Uklanjanje kolačića na web preglednicima

* Postavke – Privatnost i sigurnost – Brisanje podataka o pregledavanju
* Potrebno je to učiniti i na web preglednicima pametnih telefona
* Blokirati kolačiće treće strane, prihvaćati samo nužne kolačiće

Savjeti za sigurnost profila na društvenim mrežama

* Odaberite jaku lozinku
* Zaštitite svoj račun elektroničke pošte
* Dvostruka provjera autentičnosti
* Log-out (ako se ne logirate na svom telefonu)
* Zaštitite svoj mobilni telefon
* Pazite što klikate (lažni e-mailovi)
* Pazite na aplikacije kojima dajete pristup svom računu

Savjeti za sigurnost pametnih telefona

* Nerijetko se na mobilnim uređajima nalazi više osobnih podataka nego na stolnim i prijenosnim računalima (fotografije, videozapisi, poruke, informacije o lokaciji itd.).
* Iz tog razloga vrlo je važno podići svijest korisnika da i mobilni uređaji mogu biti pogođeni zlonamjernim sadržajem, što ugrožava korisničke podatke.
* Najpopularniji operacijski sustav je Android čiji udio na tržištu pametnih mobilnih uređaja iznosi čak 85%.
* Koristite zaključavanje zaslona
* Ne spajajte se na nesigurne mreže
* Koristite uređaje proizvođača koji redovito ažuriraju operacijske sustave
* Šifriranje pohrane podataka - koristi se mnogo kompleksniji kriptografski algoritam od samog zaključavanja zaslona. Tako su vaši podatci dodatno zaštićeni u slučaju gubitka ili krađe uređaja.

Načini predstavljanja na mreži

* Svaka se osoba na mreži može predstaviti na dva načina:
	+ svojim pravim imenom
	+ nadimkom (engl. *nickname*).
* Nadimak može biti uobičajeni nadimak koji ta osoba inače koristi ili novi nadimak osmišljen samo za tu svrhu. I pri odabiru nadimka treba razmišljati kakvu sliku šaljemo o sebi, nadimak na neki način pokazuje što mislimo ili osjećamo.
* Korištenjem nadimka na internetu smatramo da smo anonimni. To je privlačno, osobito mladim ljudima, jer omogućava slobodnije, otvorenije i intimnije izražavanje i komuniciranje.
* Ali anonimnost također omogućuje i **lažno predstavljanje**. Svatko se može predstaviti i opisati se kako god želi, a da u stvarnosti ništa od navedenoga nije istina!

Zaštite od lažnog predstavljanja nema, ali postoji pravilo:

* Na društvenim mrežama nemoj kao prijatelje dodavati ljude koje ne poznaješ!

Kako prepoznati lažni profil



Lažno predstavljanje

* Iako netko može koristiti lažne podatke pri predstavljanju, njegovo računalo uvijek je prepoznato na mreži.
* Svako računalo pri spajanju na mrežu dobije svoju**IP (*Internet Protocol*)** adresu koja ga jednoznačno određuje.
* Na mreži ne postoje dva računala s istom IP adresom.

Preporuke za sigurno predstavljanje i ponašanje na mreži



Stranice za prijavu uznemiravanja

* Red Button - online prijava zlostavljanja djeteta
* CSI – Centar za sigurniji Internet csi.hr