RADNE BELEŠKE O DIGITALNOJ BEZBEDNOSTI

DIGITALNA FEMINISTIČKA ŠKOLA 2021

DIGITALNI FEMINISTIČKI POZDRAV!

Početkom treće decenije XXI veka većina nas ne može da zamisli život bez globalne mreže, Interneta. Pandemija koronavirusa, koja nas je u fizičkom okruženju izolovala, kako bi se sprečilo širenje virusa, dovela je do toga da dobar deo našeg svakodnevnog života postane *online*. Na Internetu smo radile, studirale, kupovale, vežbale, upoznavale se, zaljubljivale, družile, posećivale koncerte i gledale filmove i pozorišne predstave. Prema podacima iz januara 2021. godine, Internet je koristilo skoro 60% globalne svetske populacije - 4.66 milijarde. Među njima, čak 4.2 milijarde je koristilo društvene mreže.

I dok nam je u *offline* svetu relativno lako da da prepoznamo koncepte bezbednosti i privatnosti, na Internetu nam to zadaje poteškoće. Dok Internetom surfujemo u svoja četiri zida, mi često mislimo da smo u tome same. Ali, to nije tačno. Sve što radimo *online*, same sa sobom, ne radimo van vidokruga drugih - apsolutna privatnost na Internetu, identična onoj u *offline* svetu, ne postoji. Svako može da sazna šta smo guglale prošlog leta, ukoliko se dovoljno potrudi. I to je tačka u kojoj se privatnost na Internetu susreće sa bezbednošću na Internetu - na nama je da im to maksimalno otežamo.

Bezbednost na Internetu ima dve komponente od kojih zavisi. Jedna se tiče tehnološke bezbednosti, odnosno uređaja koje koristimo, njihovog operativnog sistema i programa koje koristi.

Kako bismo optimizovale ovaj tehnološki aspekt bezbednosti, potrebno nam je i tehnološko znanje, koje većina nas, običnih netizenki (engl. *netizen* - korisnik ili korisnica Interneta) nema.

Na sreću, postoji još jedna komponenta bezbednosti na Internetu, koju svaka od nas može da kontrološe, a ona se tiče našeg ponašanja.

Upravo je ovo bio motiv za održavanje radionica digitalne bezbednosti koje Centar za ženske studije održava već nekoliko godina sa svojim polaznicama i polaznicima.

Druga generacija polaznica Digitalne feminističke škole (DFŠ) je ove radionice pohađala na proleće 2021. godine i upravo se na njima rodila ideja da svoja razmišljanja i zapažanja o digitalnoj bezbednosti podele sa svima koji naš jezik govore u formi ovih beležaka.

Cilj beležaka koje su pred vama, a koje su polaznice DFŠ sastavile, jeste da približe i daju osnovne smernice kako da svoje ponašanje na Internetu prilagodimo što većem nivou bezbednosti. Ove smernice nisu konačne, i sasvim sigurno su podložne zubu vremena jer se tehnologija koja digitalno okruženje gradi menja iz dana u dan. Ipak, ove smernice, iako radne i podložne stalnim dopunama, poput softvera i uređaja koje koristimo za pristup Internetu, jesu važne, jer uprkos stalnim promenama tehnologije, koncepti bezbednosti i težnje ka privatnosti na Internetu ostaju isti. Ne mora baš svako da zna šta smo, gde i sa kim guglale prošlog leta.

Hristina Cvetinčanin Knežević

04

DIGITALNI REČNIK

Privatnost na Internetu

predstavlja oblik lične privatnosti i odnosi se na pristup informacijama o nama i našem ponašanju na Internetu trećim licima.

Bezbednost na Internetu

odnosi se na zaštitu naših naloga na Internetu, uređaja koje koristimo za pristup Internetu i podataka koji se nalaze na njima kako treća lica ne bi mogla da im pristupe.

Internet pretraživač

(engl. *search engine*) je servis koji nam omogućava lakšu pretragu podataka na Internetu na osnovu zadatih termina i ključnih reči (Google, Bing, DuckDuckGo i dr.).

Internet pregledač

(engl. *Internet browser*) je program koji koristimo kako bismo pristupile sadržaju na Internetu (Firefox, Chrome, Tor, Internet Explorer, Opera, Safari i dr.).

Kolačići

su male datoteke koje se čuvaju na našem računaru kada pristupamo Internetu i omogućavaju Internet sajtovima da saznaju informacije o nama na osnovu naših Internet aktivnosti.

Digitalni otisak

(engl. *digital footprint*) predstavlja tragove koje ostavljamo za sobom prilikom korišćenja Interneta.

Oblak

(engl. *cloud*) predstavlja tehnologiju čuvanja podataka u sistemu koji se sastoji od velikog broja povezanih računara na način da nam podaci uvek budu dostupni putem Interneta, kao da se nalaze na našem uređaju.

Enkripcija

ili šifrovanje je proces u kome se podaci menjaju tako da postanu nečitljivi onima koji nemaju određeno znanje tj. ključ koji je neophodan kako bi se tim podacima pristupilo.

Metapodaci

su podaci o podacima, odnosno, informacije koje opisuju podatke. Metapodaci najčešće sadrže lokaciju, datum, vreme, vrstu uređaja i/ili softvera koji je korišćen.

Softveri

(engl. *software*) predstavljaju nematerijalne resurse koji nam omogućavaju da koristimo naše uređaje - to su programi, aplikacije, ali i sam operativni sistem.

Malveri

(engl. *malware*) predstavljaju maliciozne softvere čiji je cilj da pristupe zaštićenim podacima koji se nalaze na uređajima.

Protokoli

definišu skup pravila i procedura neophodnih za ispravan rad svih uređaja na mreži. Najpoznatiji su IP, Internet protokol, koji se odnosi na adresu našeg uređaja, i HTTP i HTTPS protokoli, koji služe za komunikaciju pregledača i sajta koji posećujemo.

Otvoren kod

(engl. *open source*) je vrsta softvera čiji je izvorni kod javno dostupan i koji svaki korisnik ili korisnica Interneta može da prilagodi svojim potrebama.

Pecanje

ili fišing (engl. *phishing*) je vrsta Internet prevare čiji je cilj krađa poverljivih informacija o nama, odnosno, našeg identiteta.

Lozinka

je skup simbola koji, u kombinaciji sa korisničkim imenom, koristimo za pristup našim uređajima i nalozima na Internetu.

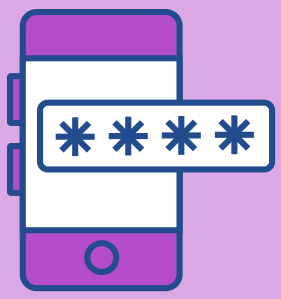
Dvofaktorska autentifikacija

ili 2FA (engl. *two-factor authentication*) je dodatni nivo zaštite u kome je, pored lozinke, za pristup nalogu potreban i unos alfanumeričkog koda koji dobijamo putem SMS poruke ili elektronske pošte.

BEZBEDNOST NA INTERNETU

odnosi se na zaštitu naših naloga na Internetu, uređaja koje koristimo za pristup Internetu i podataka koji se nalaze na njima kako treća lica ne bi mogla da im pristupe.

LOZINKE...



Lozinka je skup simbola koji, u kombinaciji sa korisničkim imenom, koristimo za pristup našim uređajima i nalozima na Internetu.

Dobra lozinka je ona koju je relativno teško pogoditi u kratkom vremenskom periodu bilo prostim nagađanjem ili upotrebom specijalizovanih softvera.

To na prvom mestu znači da bi, prilikom kreiranja lozinke, trebalo da izbegavamo da koristimo opšte pojmove, nizove reči koji se mogu naći u standardnom rečniku ili nizove brojeva, jednostavne i/ili reči koje mogu biti poznate našoj široj okolini, u kući, školi ili na poslu - na primer lozinke poput 123456, password1234, ličnog imena, imena kućnog ljubimca, partnera ili partnerke, deteta, sporta koji treniramo ili omiljenog glumca ili glumice.

Često i pored našeg truda, sajtovi i online trgovine koje posećujemo nemaju dobru zaštitu. Zato bi trebalo da koristimo različite lozinke za različita Internet mesta na kojima se prijavljujemo, kao i da ih povremeno menjamo.

Svakog dana samo Microsoft beleži preko 10 miliona napada na kombinaciju korisničkog imena i lozinke. To dosta govori o brzini računarskih operacija kojom računari sajber-kriminalaca i sajber-kriminalki danas rade.

Zato se preporučuje da naše lozinke imaju minimum 8 karaktera i obavezno uključe velika i mala slova, numeričke i specijalne karaktere, vodeći računa da cifre i specijalni karakteri ne budu na početku ili na samom kraju lozinke.

ŠTA JE *PASSPHRASE* A ŠTA LOZINKA?

Passphrase predstavlja celu frazu, rečenicu ili izraz i sastoji se od četiri pa čak i deset reči dok je loznika obično sastavljena od jedne, eventualno dve reči.

Primer *passphrase* je *DFS2021ImaSuperPolazniceKojeSuOvoPripremileZaVas* dok je primer lozinke *DFS2021carice*.

Te preporuke ponegde idu i do minimum 16 karaktera ili više, ali to ima i svoju lošu stranu – naše ponašanje postane predvidljivo, nesvesno pojednostavljujemo način šifriranja kako bismo lakše upamtili lozinku za konkretnu Internet adresu.

Pri kreiranju lozinki kao niza reči, stručnjaci i stručnjakinje upozoravaju da sajber-kriminalci i sajber-kriminalke koriste rečnike za dešifrovanje naših lozinki (engl. *dictionary attacks*), kao i da nema empirijskih dokaza da korisnici i korisnice lakše pamte *passphrase* od uobičajeno komplikovanih lozinki.

DFŠ INFO

Uputstva za pravljenje dobre loznike

- Lozinka treba da ima minimum 8 raznovrsnih karaktera koji ne bi trebalo da daju smislenu celinu;
- Lozinku ne treba da delimo sa drugim osobama niti da je zapisujemo na vidnim, lako dostupnim mestima;
- Nije preporučljivo korišćenje iste lozinke na različitim Internet sajtovima i automatsko logovanje, jer ako neko može lako da pristupi našem računaru ili telefonu, lozinka mu ni ne treba;

Kvalitet postojećih, budućih ili starih lozinki možemo proveriti ovde. Takođe na sajtu Have I Been Pwned možemo proveriti da li su neki od sajtova ili društvenih mreža koje smo koristili, ustupili naše podatke nekom drugom, ili su im podaci ukradeni, nakon čega momentalno treba promeniti lozinke.

... & MENADŽERI LOZINKI

Menadžer lozinki je softver koji omogućava jednostavnije korišćenje lozinki.

S obzirom na sve veći broj sadržaja i naloga kojim prosečni korisnici i korisnice Interneta svakodnevno pristupaju, pojavila se potreba za organizovanijom, bržom i sigurnijom opcijom od ustaljenih, često i nebezbednih načina za snalaženje u virtuelnom prostoru.

Praćenje uputstava za sigurnije kretanje Internetom podrazumeva korišćenje različitih i komplikovanijih lozinki, te menadžer lozinki može biti lako rešenje, umesto pamćenja dugih i mnogobrojnih kombinacija slova, znakova i brojeva.

Ova zgodna alatka skladišti sve lozinke na jednom mestu, daje nasumično generisane predloge i može automatski ili uz par klikova da pristupi nalogu na koji je potrebno prijaviti se. Da bi se pristupilo podacima koje čuva, neophodno je zapamtiti glavnu lozinku za sam menadžer, tzv. master lozinku (engl. *master password*) a savetuje se i dvofaktorska autentifikacija. Podaci su često enkriptovani i pohranjeni na oblaku ili na samom uređaju.

Oni koji se oslanjaju na oblak mogu funkcionisati na više platformi, te omogućuju brže korišćenje lozinki za razliku od situacije kada se lozinke čuvaju lokalno, na uređaju. Nasumično predložene lozinke za pojedinačne naloge su ne samo gotovo nemoguće za pamćenje, već komplikovane i za ručno unošenje, što upućuje da se treba potpuno osloniti na ovaj program i pamtiti samo glavnu lozinku. Osim što mogu olakšati rad, menadžeri štite od lažnih stranica koje traže lozinke (tzv. pecanje), jer neće, za razliku od korisnika ili korisnice, napraviti grešku u proceni verodostojnosti sajta.

Dostupni su različiti menadžeri koji variraju u cenama i specifikacijama: neki su besplatni, kod pojedinih su besplatne ograničene usluge (često broj lozinki u upotrebi), dok kod drugih postoje u ponudi različiti paketi. Razlikuju se i u tome koji sistem podržavaju i na kom uređaju se koriste, to jest da li se mogu koristiti na više uređaja, kao i po drugim osobinama poput mogućnosti automatskog popunjavanja (engl. *autofill*) i strategiji povratka podataka usled gubitka glavne lozinke.

Menadžeri lozinki imaju svoje prednosti i mane. Čuvanje svih lozinki na jednom mestu, osim pogodnosti, može predstavljati veliki problem ukoliko se ne prate glavne smernice upotrebe menadžera, pre svega ukoliko se ne osmisli – i zapamti – jaka glavna lozinka. Takođe treba imati na umu da, ukoliko neko drugi ima pristup uređaju, treba isključiti automatsku prijavu. Pojedini stručnjaci i stručnjakinje iz oblasti tehnologija su oprezni u korišćenju menadžera, iako se stiče utisak da je opšti konsenzus da pogodnosti prevazilaze potencijalne probleme i rizike.

DFŠ INFO

Predlozi za upotrebu menadžera lozinki

Stjuart Šehter (Stuart Schechter), istraživač u oblasti tehnološke bezbednosti, naglašava da ovi programi nisu nužno pogodni za svakog, a svakako ne za one koji ne poštuju i ne koriste njihove glavne odlike.

On daje predloge i savete koji se ukratko mogu sažeti u sledeće:

- Napraviti jaku glavnu lozinku, koju je najbolje generisati nasumično i negde zapisati dok se ne nauči upornim ponavljanjem. Nikako je ne koristiti za druge potrebe.
- Pre izbora menadžera istražiti opcije vraćanja podataka (engl. *recovery*) i podesiti opcije u programu odmah nakon određivanja glavne lozinke.
- Početi rad lozinkama koje nisu od velike važnosti dok se ne upoznaju funkcije programa.
- U skladu sa sopstvenim specifičnim okolnostima, proceniti na kojim uređajima koristiti menadžer.
- Razmisliti o tome da li čuvati lozinke visoke važnosti (menadžer se, na primer, može koristiti za generisanje lozinke bez da se ona u njemu sačuva).

Menadžer može zaštititi od pecanja, s druge strane to znači da će lozinka biti prisutna na svakom uređaju koji poseduje menadžer čineći je time osetljivijom na viruse i krađe podataka, te u tom smislu treba proceniti koji napad je verovatniji.

Naš predlog za menadžer lozinki je **Keepass**, koji je dostupan za operativne sisteme Windows, Mac OS, Android i iOS. Može se preuzeti na ovom linku.

SOFTVERI...

Softveri predstavljaju nematerijalne resurse koji nam omogućavaju da komuniciramo i koristimo naše uređaje - najčešće su to različiti programi, aplikacije, a i sam operativni sistem predstavlja softver.

Ako koristimo uređaje za pristup Internetu, svakodnevno smo pod napadom malicioznih osoba i njihovih malvera. Iako naši uređaji i softveri nisu savršeni, oni imaju svoje ranjivosti, paralelno sa ovim napadima, pojedinci i pojedinke svakodnevno rade na njihovom poboljšanju u smislu bezbednosti. Jedan od načina da se zaštitimo od ovih tehnoloških napada je i da redovno ažuriramo softvere koje korisimo, uključujući i sam operativni sistem naših uređaja. Najnovije verzije ažuriranih softvera sadrže bezbednosne zakrpe koje su tu da spreče ove napade. Stari softveri, bez novih bezbednosnih zakrpa, za maliciozne osobe prestavljaju najlakši nači da "uđu" u naš uređaj, mnogo lakši od pogađanja lozinke, na primer.

Šta je još važno kada je reč o bezbednosti softvera? Važno je da uvek koristimo legalne i najnovije softvere, pouzdanih kompanija, jer maliciozni pojedinci i pojedinke često znaju da se lažno predstave i ponude nam lažne softvere, u kojima se kriju malveri. Zbog toga softvere uvek treba da preuzimamo sa zvaničnih sajtova i naloga proizvođača u prodavnicama aplikacija.

Ukoliko nismo sigurne u pouzdanost i bezbednost nekog softvera, uvek možemo pročitati recenzije o određenom programu ili aplikaciji *online*, i u donošenju odluke o njegovom korišćenju uzeti u obzir i iskustva drugih korisnika i korisnica.

Još nešto što možemo da uradimo kako bismo poboljšali svoju bezbednost kada je reč o ažuriranju softvera da koristimo one softvere koji sami obaveštavaju korisnike i korisnice kada je dostupno novo ažuriranje, ali se ne instaliraju sami, već za to traže našu dozvolu.

... & MALVERI

Malveri predstavljaju maliciozne softvere čiji je cilj da pristupe zaštićenim podacima i informacijama koje se nalaze na uređajima.

Malveri su zbirni pojam koji označava čitav niz malicioznih softvera koje zlonamerni hakeri i hakerke koriste kako bi pristupili našim uređajima i podacima koji se nalaze na njima. Najpoznatija vrsta malvera je svakako računarski virus, ali potoje i druge vrste malvera za koje ste sigurno čule - to su trojanci, špijunski softveri (engl. *spyware*), ki logeri (engl. *key logger*) i crvi (engl. *worms*).

Malveri se šire poput zarazne bolesti - kada zaraženi uređaj dođe u kontakt sa nekim drugim uređajem, u slučaju da on nije zaštićen, zaraziće se. Malveri se najčešće šire preko zarađenih prenosnih uređaja, poput USB memorije i hard diskova, preko računarskih mreža, sajtova, elektronske pošte ali i zaraženih datoteka.

Cilj nekih malvera je da nanesu štetu uređaju ili sistemu, neki se koriste za špijuniranje i praćenje dok neki koriste podatke do kojih su došli za ucenu ili krađu (na primer - podatke o našim kreditnim karticama). Iako se po svojim ciljevima malveri razlikuju, cilj svakog malvera je da ostane skriven od nas što duže.

Iako postoje brojni anti-malver softveri, veoma često sami ne možemo u potpunosti da “očistimo” naš uređaj, te nam je potrebna pomoć profesionalaca i profesionalki.

Ipak, ono što možemo da uradimo je da ne instaliramo softvere u čiju pouzdanost nismo sigurne, da ne klikćemo na sumnjive linkove, ne otvaramo sumnjivu elektronsku poštu i da ne posećujemo nepouzdane sajtove.

DFŠ INFO

Vrste malvera

Postoji mnogo vrsta malvera, a mi izdvajamo neke od najčešćih:

Računarski virus - predstavlja mali softver koji se širi sa jednog uređaja na drugi i može da ošteti ili obriše podatke koji se nalaze na njemu. Ukoliko se umnoži u sam operativni sistem, može oštetiti neki od sistemskih datoteka i izazvati pad sistema.

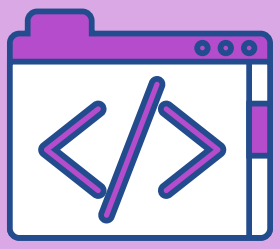
Trojanac - predstavlja malver koji se ponaša kao trojanski konj, odnosno, sakriva se unutar drugih programa. U zavisnosti od toga za šta je programiran, može naneti štetu korisnicama i korisnicima na razne načine.

Crv - predstavlja računarski kod koji se širi bez korisničke interakcije, a većina crva dolazi do uređaja preko elektronske pošte.

Špijunski malver - to je program koji prati naše navike u korišćenju uređaja i pristupu Internetu i prosleđuje ih trećim licima.

Kejloger - reč je o malveru koji prati, snima i šalje trećem licu sve što otkucamo na tastaturi.

PROTOKOLI KOMUNIKACIJE & ZAŠTITA PODATAKA



Protokoli komunikacije omogućavaju komunkaciju između pregledača i sajtova koje posećujemo a enkripcija, odnosno, šifrovanje podataka, predstavlja jedan od načina da ovoj komunikaciji ne mogu pristupiti treća lica

Sigurno ste primetile kada surfujete internetom da ispred adrese sajtova koje posećujete stoji http:// ili https://.

HTTP (engl. *HyperText Transfer Protocol*) i HTTPS (engl. *HyperText Transfer Protocol Secure*) su protokoli koji omogućavaju komunikaciju između browser-a na vašem računaru i sajtova koje posećujete tj. servera na kojima su oni pohranjeni. Svaki put kada posetimo neki sajt, naš pregledač i server sajta "pričaju" i ta komunikacija se odvija prema pravilima HTTP ili HTTPS protokola.

Kad je u pitanju HTTP protokol, naš browser i server komuniciraju običnim tekstom i naša komunikacija je dostupna svakom ko želi da je vidi. Zašto je ovo problem? Često se dešava da na sajtu ostavljamo naše lične podatke i šifre kada im pristupamo ili brojeve kartica kad kupujemo *online*. Ovi podaci su čitljivi svakom ko presretne našu komunikaciju i mogu biti zloupotrebljeni. Čak i ako ne ostavljamo svoje podatke, svakako ostavljamo informacije o tome šta nas je zanimalo i šta smo pretraživali. Zato se HTTP protokol sve više zamenjuje HTTPS protokolom.

Kao što smo već pomenule, slovo "S" u HTTPS označava secure, tj sigurano. Ovaj protokol obezbeđuje bezbednu vezu našeg pregledača sa serverom sajta tako što obavlja enkripciju.

Osim što mogu olakšati rad, menadžeri štite od lažnih stranica koje traže lozinke (tzv. pecanje), jer neće, za razliku od korisnika ili korisnice, napraviti grešku u proceni verodostojnosti sajta.

ŠTA JE ENKRIPCIJA?

Enkripcija ili šifrovanje je proces u kome se podaci menjaju tako da postanu nečitljivi onima koji nemaju određeno znanje tj. ključ. Da bi ovi podaci bili razumljivi moraju se dešifrovati pomoću ključa. Enkripcija je važna jer bi bez nje naši osetljivi podaci bili lako pročitani i izloženi krađi i zloubotrebi. To može dovesti do krađe identita, finansijske prevare ili neke druge lične štete.

Pregledači prepoznaju razliku među protokolima HTTP i HTTPS i na adresnoj traci (engl. *address bar*) nas obaveštavaju koja vrsta protokola je u pitanju. Ako je sajt bezbedan tj. koristi HTTPS protokol, ispred imena protokola videćemo katanac.

Danas HTTPS protokol postaje standard. Google, najveći pretraživač, prednost daje sajtovima koji koriste HTTPS protokol i time primorava većinu sajtova da pređu na bezbedniji protokol. Svi zastupljeniji pregledači (Chrome, Firefox, Opera) takođe usmeravaju sajtove ka prelasku na HTTPS protokol tako što nas obaveštavaju kada pristupamo nebezbednim sajtovima ili nam blokiraju pristup.

DFŠ PREPORUKA

HTTPS Everywhere

Naša preporuka za obezbeđivanje sigurne konekcije je **HTTPS Everywhere**. On je besplatni softver otvorenog koda koji može dodatno da nas zaštiti.

Kada instaliramo HTTPS Everywhere na naš pregledač, on će automatski pretvarati vezu sa sajtom u sigurnu vezu. Mnogi sajtovi nude ograničenu mogućnost šifrovanja komunikacije npr. podrazumevano vas vode na HTTP verziju sajta ili vas sa šifrovanih delova sajta linkovima vode ka nešifrovanim delovima. HTTPS Everywhere prisiljava svaki sajt koji podržava HTTPS protokol da ga koristi u komunikaciji sa vama.

Instalacija HTTPS Everywhere ekstenzije ne znači da će vaša komunikacija sa sajtovima baš svaki put biti šifrovana, jer postoje sajtovi koji i dalje nisu prešli na HTTPS protokol. Dakle, ova ekstenzija koristi već postojeće sigurnosne funkcije sajtova i ne može ih stvoriti ako već ne postoje. Ako želite da u potpunosti odbijete svaku nešifrovanu komunikaciju, HTTPS Everywhere vam i to omogućava odabirom opcije “encrypt all sites eligible”.

Ovde je još bitno pomenuti i koje podatke HTTPS Everywhere ne štiti. HTTPS Everywhere ne krije identitet sajtova kojima pristupate, količinu vremena koje provodite koristeći ih ili količinu informacija koje šaljete ili preuzimate sa određenog sajta. Ako se želite zaštititi od praćenja sajtova koje posećujete, razmislite o korišćenju HTTPS Everywhere zajedno sa softverom poput Tora.

Instalaciji HTTPS Everywhere ekstenzije možete pristupiti preko ovog linka.

DVOFAKTORSKA AUTENTIFIKACIJA

Dvofaktorska autentifikacija ili 2FA je dodatni nivo zaštite naših naloga na Internetu.

Ona nam omogućava da prilikom pristupanja određenom sistemu neće biti dovoljno da se unesu samo korisničko ime i šifra, nego će se zahtevati alfanumerički kod, koji će nam biti poslat SMS-om, a koji ćemo morati uneti da bi verifikovali svoj identitet.

Stoga, ako neko želi da hakuje naš nalog na određenoj društvenoj mreži to neće moći da obavi ukoliko nema pristup i našem mobilnom telefonu.

TIPOVI DVOFAKTORSKE AUTENTIFIKACIJE

Postoje četiri tipa dvofaktorske autentifikacije:

1) Informacija koju zna samo vlasnik tj. vlasnica naloga, poput odgovora na sigurnosno pitanja, PIN-a ili lozinke.

2) Nešto što poseduje vlasnik/ca naloga, sigurnosni token, identifikacijski dokument ili mobilni uređaj.

3) Biometrijska provera, odnosno otisak prsta, prepoznavanje lica ili glasa.

4) Lokacijska provera, koja označava mesto sa kog se vrši autentifikacija, poput IP adrese ili geografskog izvora.

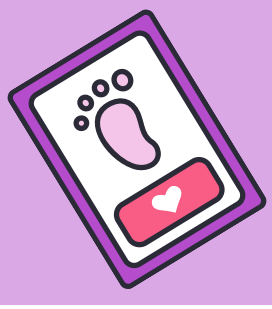
Dvofaktorska identifikacija predstavlja pojačanu sigurnost našeg naloga. Kao što i samo ime kaže, dva faktora autentifikacije su veća zaštita od samo jednog faktora. Jedan faktor zaštite predstavlja lozinka koju korisnik/ca izabere, ona iako može biti poprilično jaka, za dobrog hakera ili hakerku ne mora predstavljati veliki problem.

U tim situacijama dvofaktorska autentifikacija može biti vrlo značajna. Iako je dvofaktorska autentifikacija uglavnom opcionog karaktera, svaka društvena mreža (Instagram, Facebook, Twitter, Google, LinkedIn i dr.) nudi svojim korisnicima tu mogućnost i na taj način poboljšavaju korisničko iskustvo i smanjuju rizik da neko neovlašćeno pristupi našem nalogu.

PRIVATNOST NA INTERNETU

predstavlja oblik lične privatnosti i odnosi se na pristup informacijama o nama i našem ponašanju na Internetu trećim licima.

POSTOJI LI PRIVATNOST NA INTERNETU?



Digitalni otisak (engl. *digital footprint*) predstavlja tragove koje ostavljamo za sobom prilikom korišćenja Interneta.

U poslednje vreme, među korisnicima i korisnicama Interneta javlja se zabrinutost zbog privatnosti podataka koje razmenjujemo, koja uključuje pitanja ko sve sakuplja te podatke, da li se nesvesno podeli mnogo više podataka od željenih i, na kraju, za šta se ti prikupljeni podaci kasnije koriste.

Kada govorimo o privatnosti u kontekstu mrežnih komunikacija, zapravo mislimo na mogućnost da pojedinac/pojedinka kontroliše podatke koje deli, kao i na one koje ostavlja za sobom u obliku digitalnog traga, digitalnog otiska (engl. *digital footprint*).

Gotovo svakodnevno obaljamo razne kupovine online, pretplate na multimedijalne sadržaje, prihvatamo razne kolačiće, oglase i ne sluteći da se, nesvesno, izlažemo rizicima povrede naše privatnosti, ali i brojnim drugim sigurnosnim rizicima. Shvativši kakvim su rizicima izloženi korisnici i korisnice, stručnjaci i stručnjakinje su počeli razvijati brojne alate i metode koji doprinose našoj “anonimizaciji“, odnosno čuvaju pravo na našu privatnost na Internetu.

PRETRAŽIVAČI & PERSONALIZOVANA PRETRAGA

Internet pretraživači (engl. *search engines*) su servisi koji nam omogućavaju lakšu pretragu podataka na Internetu na osnovu zadatih termina (engl. *search query*).

Rezultati ove pretrage su uglavnom prezentovani kroz desetak linkova i drugih vrsta podataka kao što su fotografije, video klipovi i sl.

Neki od najpoznatijih pretraživača su Google, Sogou, Baidu, Bing, DuckDuckGo i Yandex. Jedna od glavnih tema kada su u pitanju pretraživači jeste privatnost korisnika i korisnica. Sposobnost pretraživača da prikuplja podatke o korisnicima i korisnicama i, na osnovu toga, personalizuje pretragu, zabrinjavajuća je zbog mogućnosti zloupotrebe podataka, kao i zbog nedostatka jasne zakonske regulative.

Personalizovana pretraga je pretraga specifično kreirana za svakog korisnika i korisnicu pomoću algoritma koji "zna" šta korisnika/cu zanima, a zasnovano na infomacijama kao što su lokacija, jezik i istorija pretraga (engl. *search history*).

Pionir personalizovane pretrage je Google (Google) koji je ovu mogućnost uveo 2004. godine. Ovakva pretraga daje mogućnost da se rezultati prilagode interesovanjima korisnika uz pomoć anonimnog kolaćića u vašem pretraživaču, čak i kada nismo ulogovani na Google naloge (Gmail, YouTube, itd.).

Ukoliko smo ulogovane na naše naloge, ovakva pretraga je još više prilagođena, a Google-ov glavni argument je da žele svojim korisnicima i korisnicama da pruže najrelevantnije moguće podatke.

Ono što svakako možemo uraditi kako bismo što više zaštitili svoju privatnost je da prestanemo da koristimo Google i počnemo da koristimo neki od pretraživača koji ne upotrebljava podatke o korisnicima i korisnicama.

DFŠ INFO

Kako isključiti personalizovanu pretragu na Google nalogu?

Personalizovanu pretragu na Google nalogu možemo isključiti u nekoliko lakih koraka:

1) Ulogujemo se na svoj Google nalog
2) U donjem desnom uglu kliknemo na Podešavanja (*Settings*)
3) Odaberemo Podešavanja pretrage (*Search Settings*)
4) Kada se otvori nov prozor, kliknemo na Privatne rezultate (*Private results*).
5) Zatim kliknemo na dugme pored Privatnih rezultata.

Iako možemo da ugasimo personalizovnu pretragu, Google i dalje može prilagoditi pretragu na osnovu lokacije i drugih faktora.

DFŠ PREPORUKA

DuckDuckGo za pretraživanje Interneta

Naša preporuka je **DuckDuckGo** (DDG), pretraživač koji postoji od 2008. godine. Osnovao ga je Gabrijel Vajnberg (Gabriel Weinberg) u Pensilvaniji. Osnovna odlika ovog pretraživača i ono na čemu kompanija najviše insistira je privatnost korisnika. DDG nastoji da zaštiti privatnost korisnika i korisnica, i da izbegne tzv. pročišćen mehur (engl. *filter bubble*) odnosno personalizovane rezultate pretrage. Glavna politika privatnosti ovog pretraživača je da ne prikupljaju i ne dele informacije korisnika. DDG ne čuva IP adrese, ne evidentira korisničke podatke i koristi samo neophodne kolačiće.

Glavne razlike između DDG i Google pretraživača su u sledećem:

Reklame - Za razliku od Google-a koji prati sve naše pretrage, čuva podatke, a potom na osnovu tih podataka prikazuje reklame namenjene baš nama, u DDG ističu da su reklame na njihovom pretraživaču povezane isključivo sa terminom konkretne pretrage, a ne sa prikupljenim podacima.

Recimo, ukoliko pretražujete automobile, prikazivaće vam se reklame o automobilima.

Rezultati pretrage - U slučaju Google-a, kao što je već spomenuto, rezultati pretrage su personalizovani na osnovu naših prethodnih pretraga i interesovanja, kao i na osnovu lokacije. Glavni argument za to je relevantnost podataka. Međutim, DDG objašnjava da nije potrebno pratiti korisnike kako bi mu se pružili relevantni podaci vezani za lokaciju, kao što je vremenska prognoza. Uređaj koji koristite već sadrži infomacije o lokaciji na osnovu koje se mogu dati adekvatni podaci bez praćenja.

Ono što je još opasnije je tzv. pročišćen mehur, odnosno, ukoliko imamo određene političke stavove ili npr. stav o vakcinaciji, što je trenutno jako važna tema, mnogo je veća verovatnoća da ćemo dobijati rezultate koji su u skladu sa našim stavovima, i da ćemo veoma retko nailaziti na rezultate koji su u suprotnosti sa našim mišljenjem. Na taj način, dobijamo potvrdu naših stavova jer mislimo da su rezultati isti za sve, i ostajete u našem mehuru.

DDG daje nepristrasne rezultate i ne filtrira ih na način koji će onemogućiti da dođemo do razno-vrsnih informacija na određenu temu.

“Ekosistem” - Još jedna stvar koju Google praktikuje je da nas usmerava na svoje proizvode, pa se tako stalno vrtimo u njihovom tzv. “ekosistemu”. Osim samog pretraživača, Google takođe ima i servise kao što je npr. Google Finance, Google Flights, Google News i drugi, i uvek će favorizovati svoje servise u rezultatima pretrage. DDG će nam jednostavno prikazati rezultate kojima raspolaže jer nemaju ovakav skup svojih proizvoda.

Ukoliko koristimo Google Chrome za pretragu, donekle se možemo zaštititi tako što ćemo dodati DDG ekstenziju za Chrome. Ova ekstenzija pomaže da vaši lični podaci ne budu prikupljeni i zloupotrebljeni. DuckDuckGo možemo koristiti i na svom telefonu tako što jednostavno instaliramo aplikaciju iz Play ili App Store-a.

PREGLEDAČI & PRIVATNOST NA INTERNETU

Internet pregledači (engl. *web browsers*) su programi koji koristimo kako bismo pristupili sadržaju na Internetu (Firefox, Chrome, Internet Explorer, Opera, Safari i dr.)

Kada god pristupimo Internetu, koristeći pregledač, mi za sobom ostavljamo digitalni trag, odnosno, otisak, koji omogućava naše praćenje - nije neophodno da koristimo Google servise, poput personalizovane pretrage, za to. Većina komercijalnih sajtova ima instaliran neki od alata koji im pomaže da prikupe veoma detaljne podatke o svojoj ciljanoj publici. Ovi podaci kasnije se koriste prilikom kreiranja reklama i targetovanja potrošača. Jedan od ovih servisa predstavlja i Google Analitika (Google Analytics).

Kako nas sajtovi “prate”? Tako što koriste kolačiće.

Kolačić je mali podatak, veličine oko 4 KB, koji server šalje korisnikovom Internet pregledaču. On se uglavnom koristi za upravljanje sesijama, personalizaciju ali i praćenje i dokumentovanje korisničkog ponašanja na Internetu.

Po pravilu, kolačić nikada ne bi trebao sadržati osetljive podatke jer ne postoji sigurna zaštita koja bi zaštitila njegov sadržaj. Svaki od kolačića ima svoj domen. Ako je domen jednak domenu stranice na kojoj se korisnik nalazi, onda je reč o kolačiću prve strane (engl. *first-party cookie*). Kada se domeni ne poklapaju, onda je to kolačić treće strane (engl. *third-party cookie*). Kolačići prve strane šalju se stranici koju korisnik pregleda, dok se kolačići treće strane koriste u svrhu oglašavanja i praćenja korisnika na Internetu. Kolačiči trećih strana prisutni su na velikom broju sajtova koje posećujemo i deluju invazivno na našu privatnost.

DFŠ PREPORUKA

Tor i Privacy Badger

Postoji barem dva načina da osujetimo praćenje na Internetu i poboljšamo našu privatnost - koristeći bezbedne pregledače i koristeći ekstenzije koje onemogućavaju praćenje. DFŠ preporuka su korišćenje pregledača **Tor** ili korišćenje ekstenzije **Privacy Badger**.

Tor je pretraživač koji koristi tzv. onion routing i trenutno je najstabilnija implementacija onion mreže. Onion routing je naziv za tehnologiju anonimne komunikacije putem računarskih mreža. U onion mreži, poput slojeva luka, poruke su spakovane u slojeve enkripcije. Podaci se prenose nizom mrežnih stanica, tj čvorova, od kojih je svaka zadužena za jedan sloj zaštite, otkrivajući jedino sledeću destinaciju podataka. Kada je poslednji sloj uspešno dešifriran, podaci bivaju dostavljeni na odredište. Poslednja stanica jedina zna sadržaj poslatih podataka, ali ne i pošiljatelja, čime se postiže anonimnost u ovoj mreži.

Motivi za korišćenje Tor-a, koji, prilikom surfovanja, distribuira naš dolazni i odlazni promet kroz niz virtualnih tunela i na taj način štiti našu privatnost, mogu biti raznoliki.

Koriste ga i svakodnevni korisnici i korisnice Interneta kada žele doći do sajtova koje su ograničene od strane provajdera, dok neki biraju da Tor koriste u ilegalne i negativne svrhe. Ipak, većina korisnika i korisnica jednostavno želi da zaustavi sajtove od praćenja svakog njihovog poteza ili određivanja njihove geolokacije.

Koncept Tor-a, kao i konfiguriranje računara za slanje i primanje paketa u mreži, postaje sve raširenije i prihvaćenije širom sveta. Ako odaberemo "Tor Browser Bundle" programski paket, dobićemo najlakšu verziju instalacije, koja zahteva naše minimalne intervencije prilikom instalacije. Programski otvoreni kod Tor-a, u kombinaciji sa modifikovanom verzijom Mozilla Firefox pregledača, nudi mogućnosti da Tor Browser Bundle instaliramo na Windows, Mac i Linux platformama, po našoj želji.

Privacy Badger je besplatna i otvorena ekstenzija koja nas čuva od različitih dodataka za praćenje (engl. *tracker*) i to nam daje na znanje svaki put kada pretražujemo neki sadržaj na Internetu. On automatski ograničava praćenje dodataka (engl. widgets) društvenih mreža, kao što je Facebook-ovo dugme "like", omogućava korisnicima i korisnicama da "lajkuju" ono što žele ali sprečavaju društvenu

mrežu da prati čitalačke navike korisnika i korisnica. Privacy Badger takođe blokira praćenje oglasnih mreža uz pomoć kolačića.

Namena Privacy Badger-a nije da u potpunosti blokira, već da zaštiti privatnost Internet korisnika/ca tako što će zaustaviti prikupljanje informacija o stranicama koje osoba posećuje. Dakle, glavna karakteristika ovog alata jeste da, blokirajući oglase i reklame, koji su samo vrh „ledenog brega“, čuva i našu privatnost. Kada Privacy Badger vidi isti dodatak za praćenje na tri različite stranice, on ga blokira i mi postajemo nevidljivi za oglašivača. Ipak, on nije blokator reklama (engl. *ad blocker*).

Blokatori reklama su ekstenzije koje efikasno blokiraju agresivne reklame na sajtovima koje posećujemo, HTML elemente, frejmove, fotografije i druge neželjene sadržaje, a za njihovo korišćenje nije potrebno nikakavo dodatno podešavanje ili predznanje. Dok oni služe za smanjenje nereda na web stranicama i izbegavanje oglasa zaraženih softverskim virusom, Privacy Badger automatski blokira nevidljive dodatke za praćenje na temelju njihovog ponašanja.

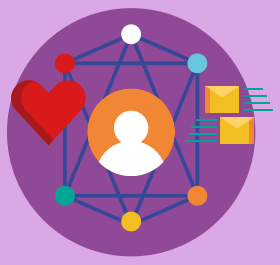
Privacy Badger radi tako što šalje *Do Not Track Signal* različitim kompanijama da nas ne prate. Ukoliko te kompanije ignorišu naše želje, Privacy Badger će znati kako ih blokirati bilo da se radi o oglašivačima ili dodacima za praćenje druge vrste. Privacy Badger je tu da primora kompanije da poštuju želju korisnika i korisnica da ne budu praćeni.

Privacy Badger ekstenziji možete pristupiti ovde a dostupan je za pregledače Firefox, Opera i Microsoft Edge.

PRIVATNOST NA DRUŠTVENIM MREŽAMA

Pics or it didn’t happen!

POSTOJI LI PRIVATNOST NA DRUŠTVENIM MREŽAMA?



Društvene mreže predstavljaju online servise koji pružaju i nude razne mogućnosti povezivanja i komunikacije sa korisnicima i korisnicama širom sveta, kao i raznolike mogućnosti lične prezentacija.

Razvoj ličnih kompjutera (PC) koji je počeo tokom 90-tih godina XX veka doveo je do njihovog umrežavanja, što je, postepeno, dovelo do stvaranja prvih društvenih mreža. Iako su u početku bile profesionalne, brzo se uvidelo da je moguće njihovo korišćenje i širenje i van stručnih krugova. Početkom XXI veka dobili smo društvene mreže koje koristimo i danas.

Među najpopularnijim mrežama sa najviše korisnika i korisnica širom sveta su Facebook, Twitter, YouTube, LinkedIn, Twitter, Instagram, Pintrest, WhatsApp, Viber, SnapChat, TikTok, Tumblr... ali ima dosta i onih (Qzone, Weibo, Taringa, Odnoklassniki, Mixi...) koje su zastupljenije u nekim regijama sveta, ali nisu rasprostranjene kao ove prethodno pomenute.

S obzirom na brzinu kojom živimo, mreže nam omogućavaju brzu i jednostavnu komunikaciju, koja se odvija u realnom vremenu. Povezale su ljude svih nacionalnost i jezika koji se nikad ne bi upoznali, uzrasta, društvenih klasa i slojeva, političkih opredeljenja, seksualnih opredeljenja, nivoa obrazovanja, religija i veroispovesti, profesija i zanimanja sa svih meridijana. Mreže su, takođe, stvorile zajednice kojima pripadamo, a da toga i ne moramo biti svesni, ili nam to ne mora biti važno. Jednom rečju, pokazale su i dokazale da zaista živimo u „globalnom selu“.

Danas se može reći da osoba koja nije na mrežama i ne postoji, kao i da se, ono što nije „okačeno“ na mreže, nije ni desilo. Fraza „Pics or it didn't happen“ je već ušla u sve urbane rečnike i postala je imperativ kojem se mnogo ljudi pokorava.

Statistike kažu da:

- 3,96 milijardi ljudi u svetu koristi društvene mreže što je skoro duplo više u odnosu na 2015. kada je taj broj bio 2,07 milijardi.
- U proseku u 2020., svaka osoba ima po 8,6 naloga naloga na mrežama, dok je taj broj bio 4,8 u 2014. godini.
- 50,64% od 7,77 milijarde ljudi širom sveta koji imaju profile na mrežama je starije od 13 godina, 63% su aktivni korisnici
- Od skoro 4 milijarde korisnika društvenih mreža, 99% pristupa sajtovima ili aplikacijama preko mobilnih telefona a samo 1,32% preko desktop računara.
- Globalno govoreći, prosečno vreme koje osoba provede svakog dana na mrežama je 2 sata i 24 minute: ako neko napravi profil sa 16 godina i živi do 70., tokom života će na mrežama provesti 5,7 godina svog života.

Takođe se može reći da naši telefoni, uređaji preko kojih najčešće pristupamo društvenim mrežama, u čak 98,8% slučajeva, znaju sve o nama. Oni znaju skoro sve, od toga koliko spavamo i kada ustajemo, koliko smo kog dana i čega pojele a i koliko smo prešle peške, znaju koliko smo novca potrošile i koliki nam je bankovni limit, do toga koje smo sajtove posetile. Znaju sa kim smo sve pričale i o čemu, kao i to kakve smo fotografije poslale i primile. Znaju adrese na kojima smo fizički bile, kao i na koje smo poslale svoj CV u nadi da ćemo naći bolji i perspektivniji posao ili da ćemo dobiti školarinu koju odavnu priželjkujemo.

Tehnologija, Internet i mreže su nam stavile svet na dlan i bitno nam olakšale život do te mere, da vrlo često, očarani svime što dobijamo, zaboravljamo da sve ima i svoju drugu, tamnu stranu.

Dve su stvari, sa te druge strane, krucijalne: gubitak privatnosti i razvoj zavisnosti od socijalnih mreža.

S obzirom na to šta sve pohranimo u vlastitim online špajzima, kao što su Drive, DropBox i slično, kao i na mrežama na kojima imamo otvorene profile, gubitak privatnosti, ako o tome ne vodimo dovoljno računa, je više nego izvestan. A gubitak naše privatnosti uvek povlači i gubitak privatnosti drugih, jer smo umreženi sa mnogima. Ko dođe do naše privatnosti, došao je i do privatnosti svih onih sa kojima smo povezani. Dakle, pošto smo ubedile sebe da bez Interneta i mreža više ne možemo da živimo i funkcionišemo, postavlja se pitanje: kako da uredimo virtuelni svet da bi u njemu bile bezbedne?

Dok većina nas razmišlja o tome šta pišemo i koje fotografije i video zapise delimo na društvenim mrežama, mali broj nas razmišlja o tome da, često nesvesno, delimo i našu fizičku lokaciju.

GEOOZNAČAVANJE

Geooznačavanje (engl. *geotagging*) predstavlja postupak tokom kojeg se različitim medijima, kao što su fotografije, video zapisi, objave na mrežama i sl., dodaju geografske identifikacije, a koje ukazuju na tačnu fizičku lokaciju osobe koja je to objavila.

Ova funkcija nije nešto novo na Internetu pa je ima većina društvenih mreža i koristi je većina aplikacija koje imamo na telefonima i tabletima. Ovu opciju imaju i fotoaparati kao i videokamere.

Kao i sve, ima dobre i loše strane. U dobre možemo navesti to da nam geooznačavanje može pomoći pri istraživanju nekog mesta ili lokacije, tako što ćemo pročitati iskustva onih koji su tamo bili pre nas pa su objavili svoje utiske, a okačili su i poneku fotku. Geolokacija nam pomaže da se povežemo sa ljudima koji pružaju određene usluge za koje smo zainteresovani, kao što su, na primer, časovi urdua ili keramičarski radovi. Takođe, ako se u nekoj gužvi, na nekom koncertu ili protestu, razdvojimo od društva sa kojim smo došli, najlakše ćemo se pronaći ako jedni drugima pošaljemo svoje lokacije.

Sa druge strane, deljenje lokacije može biti opasno ako naša adresa padne u pogrešne ruke ili ako se nadamo da ćemo ostati anonimni na mrežama.

Nesmotreno, ako objavimo svoju lokaciju, reći ćemo drugima da smo negde gde ne bismo smeli biti, na primer: ako smo navodno bolesni a objavljujemo da smo na lokalnoj plaži. Situacija može biti i opasnija: geooznačavanje nas takođe može dovesti i u opasnost ako nas neko prati, jer bi naša redovna ažuriranja postova na društvenim mrežama omogućila progonitelju da nas prati.

Posebno je važno naglasiti da kačenje fotografija dece na društvene mreže sa geolokacijom može biti izuzetno opasno, s obzirom da je poznato da velik broj pedofila odabira svoje žrtve preko Interneta i pravi mreže sa drugim pedofilima, deca lako mogu postati plen a da to niko ni ne primeti.

Ne manje bitno jeste i to što označavanjem svoje lokacije, možemo dovesti u opasnost i nekog drugog: na primer, nekog ko je sa nama, a ne želi da se javno zna gde je. Geooznačene fotografije prate i lovokradice u Africi i pomoću njih pronalaze životinje u rezervatima koje potom ubijaju i prodaju. Zato se turistima objašnjava kako da isključe sve opcije i funkcije telefona i fotoaparata koje omogućavaju geolokaciju.

Nisu samo životinje u opasnosti: geotagovi određenih krajolika privlače sve više posetitelja i turista koji ih svojim prisustvom upropaštavaju i dovode u ekološku opasnost. To se dogodilo sa jezerom Delta koje je na zabačenom mestu na Grand Tetansu, koje je odjednom postalo popularno i bilo preplavljeno turistima.

Uključenom geolokacijom, dok smo na letovanju možemo skrenuti pažnju lopovima da nismo kod kuće i da je ona prazna, pa im tako olakšati posao da nam opljačkaju sve što imamo.

Sve što treba da učinimo da bismo se zaštitili od ovih opasnosti jeste da uklonimo geotagove tako što ćemo ih ukloniti alatom za uklanjanje metapodataka. Ipak, od uklanjanja metapodataka koji sadrže informacije o našoj lokaciji, lakše je isključiti lokaciju na našem telefonu i ne deliti fotografije za koje nismo sigurne da želimo da ih baš svi vide, pa čak i one vrlo zlonamerne osobe, poput lopova.

DFŠ INFO

Kako ukloniti lokaciju sa telefona?

Kada je na našem telefonu uključena lokacija, možemo dobiti informacije na osnovu njegove lokacije, poput predviđanja putovanja na posao, obližnjih restorana i boljih rezultata lokalne pretrage.

Kada aplikacija koristi lokaciju našeg telefona putem GPS-a, na vrhu zaslona prikazuje se lokacija.

Kako da uključimo ili isključimo lokaciju na svom Android telefonu:

1) Prevučemo prstom od vrha zaslona prema dole
2) Dodirnemo i zadržimo lokaciju kako bismo je isključile ili uključile

Ako imamo iPhone i želimo da usključimo geolokaciju, treba da:

1) Idimo na početnu stranicu našeg iPhone-a i dodiremo Postavke (*Settings*)
2) Kliknemo Privatnost (*Privacy*)
3) Pritisnemo Usluge lokacije (*Location services*) i uključimo ili isključimo
4) Pregledamo popis aplikacija od vrha do dnu i potražimo željenu aplikaciju.
5) Dodirnemo je i odaberemo hoćemo li deliti svoju lokaciju dok koristimo aplikaciju, nikad ili da nas uređaj pita sledeći put. Učinimo isto za ostale aplikacije.

Na sličan način mogu se isključiti geolokacije i sa fotoaparata i videokamera.

HOMO INTERNETICUS

Šta kada nestane wi-fi?

HOMO INTERNETICUS

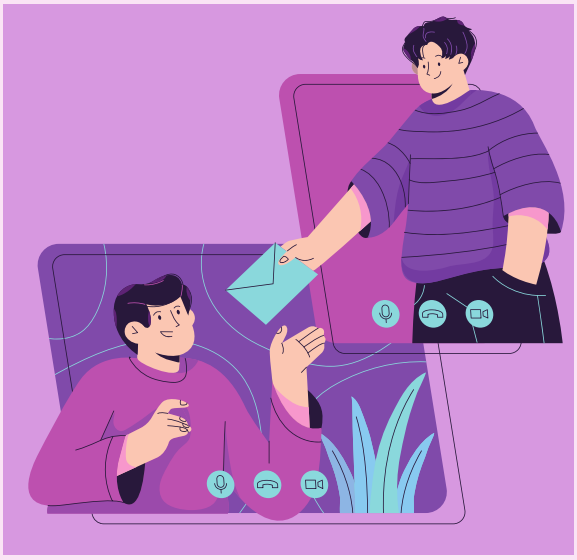
Digitalne tehnologije su izmenile način na koji živimo, jer je deo našeg života postao online: ujutro nas budi alarm sa telefona koji zahvaljujući Internetu prati astronomsko vreme, nakon čega počinje naš dan koji nam organizuju, uređuju i olakšavaju brojne aplikacije.

One nas podsećaju da ujutro treba odmah da popijemo čašu vode ili neki lek, broje kalorije našeg doručka, opominju koje obaveze imaju naša deca, zovu nam taksi ili ukazuju koliko treba da čekamo na gradski autobus koji će nas prebaciti do posla, podsećaju nas na sve obaveze koje tog dana imamo u kancelariji, od sastanaka preko telefonskih poziva koje treba da obavimo, do rokova koje nikako ne smemo "probiti“ i elektronske pošte na koje moramo odgovoriti. Tehnologija nam omogućava korišćenje alata za pisanje, crtanje, slikanje, snimanje, fotografisanje, kao i uređivanje, ispravljanje i korigovanje svega što smo uradili.

Nakon posla i profesionalnih obaveza, pomoću Interneta i društvenih mreža razgovaramo sa članovima i članicama porodice i prijateljima, bilo da žive dve ulice od nas ili na drugom kraju sveta. Tehnologija je tu da nas podseti kad je kome od ljudi koje poznajemo rođendan (ili neki drugi važan datum) i da nam pomogne da ga čestitamo ili čak i da izaberemo poklon. Preko Interneta kupujemo najrazličitije stvari i za sebe, koje onda možemo pratiti na njihovom putovanju od nekog magacina, u, na primer Velingtonu na Novom Zelandu, sve do naših vrata na koja će poštar ili poštarka da nam donese paket. Kad nas mrzi da kuvamo, naručimo hranu online, pa nam je donesu gotovu.

Telefon, tablet ili računar nam pomaže da se permanentno obrazujemo i usavršavamo i da pomoću njih pohađamo časove i kurseve, kako neke neobavezne, kao što je, na primer, kuvanje ili ples, pa sve do kurseva nekih od najpoznatijih svetskih univerziteta.

Preko Interneta otkrivamo i učimo jezike i usavršavamo one koje već govorimo, a preko mreža nalazimo društvo sa kojim ćemo taj jezik uvežbavati. Pružaju nam mogućnost pretraživanja velikog broja virtuelnih biblioteka i preuzimanja knjiga, naučnih radova i članaka iz najrazličitijih mogućih oblasti.



Aplikacije nam omogućuju pristup bankovnom računu, pa tako plaćamo račune bez da čekamo u dugim redovima dok ne dođemo do šaltera na kojem ćemo platiti sve dažbine. Omogućuju nam i da podignemo kredit (i potrošimo sve pare), bez da smo kročili u banku ili izašli iz svoje spavaće sobe.

Neke druge aplikacije nam pomažu da vodimo računa o svom zdravlju, pa nas podsećaju da treba da pijemo vodu na svaka dva sata, kao i o svojoj kondiciji i broje nam korake koje smo napravile, izračunavaju nam visinsku razliku koju smo savladale tokom pešačenja, izmišljaju sve moguće vidove aktivnosti koje možemo da zamislimo kao rekreaciju, a na kraju dana nas i nagrade nekim virtuelnim peharom kad ostvarimo vlastiti rekord, sve u nadi da će nas tako motivisati da nastavimo sa vežbanjem.

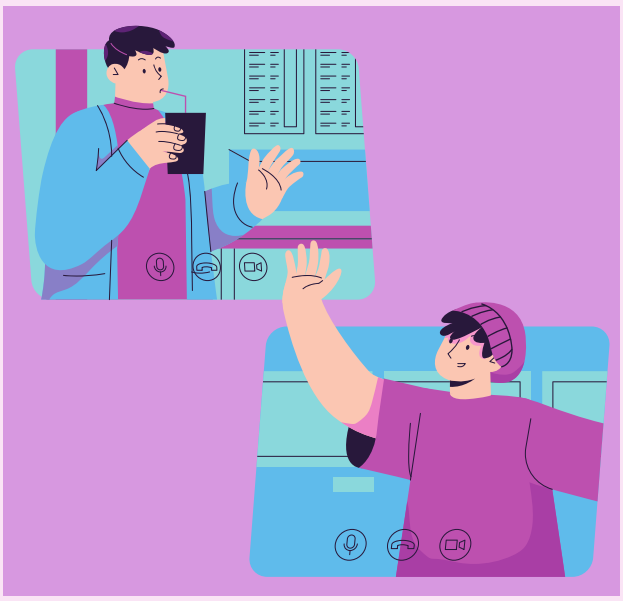
Nadalje, preko Interneta se informišemo o političkim zbivanjima, čitamo vesti, komentarišemo zbivanja i događaje, raspravljamo se sa neistomišljenicima i vodimo virtuelne krstaške ratove, učestvujemo u raznim anketama i istraživanjima javnog menjenja.

Virtuelno tražimo sledeću destinaciju na koju ćemo putovati, čitamo blogove i gledamo vlogove, tražimo fotografije ljudi koji su tamo već boravili i gledamo kako su ocenjivali mesta koja nas zanimaju. Aplikacije nam nude i avio-karte i hotele i taksi prevoz do hotela, pa mi samo treba da spakujemo kofer i siđemo ispred kuće da nas taksi pokupi i odveze do aerodroma.

Preko aplikacija upoznajemo potencijalne partnere i partnerke, četujemo do besvesti sa onima sa kojima mislimo da imamo nešto zajedničko. Virtuelno se i zaljubljujemo, pa se tek posle toga upoznajemo sa osobom od "krvi i mesa“. Aplikacije nas obaveštavaju kada su nam plodni dani i koliko je dana do početka sledećeg ciklusa, a nekad nam stvaraju paniku kad nas obaveste da nam ciklus kasni.

Opominju nas kada treba da odemo kod zubara/ke ili ginekologa/škinje na kontrolu. Internet nam omogućava da nađemo stan ili kuću u kojoj ćemo sa partnerom ili partnerkom živeti "sretno i zadovoljno do kraja života“, a pomaže nam i da isplaniramo i organizujemo "naše venčanje iz snova“. Ako stvari ne krenu kako treba, preko Interneta možemo naći i dobru/og advokata/icu koji će nas razvesti, pa onda možemo sve ponovo.

Pomoću aplikacija ograničavamo, usmeravamo, nadziremo i kontrolišemo sadržaje kojima naša deca pristupaju preko svojih pametnih telefona i tako ih štitimo, a nekad, istini za volju, i, pomalo, špijuniramo. Ograničavamo im vreme za igrice i pokušavamo da ih usmerimo na edukativnije sadržaje. Gledamo s kim se druže online i u koje grupe ulaze, te koje sajtove posećuju i koliko na njima provode vremena. Internet je sjajno mesto da se zadovolje dečija i mladalačka radoznalost i želja za učenjem i otkrivanjem novih stvari i horizonata, ali je u isto vreme i izuzetno opasno mesto, ako deca i mladi ne znaju kako da ga bezbedno koriste.



Podaci UNICEF-a pokazuju da: više od dve trećine dece i mladih (74%) ima profil na nekoj društvenoj mreži ili platformi za igranje video igara - od toga, 41% njih uzrasta 9-10 godina kao i 72% njih uzrasta 11-12 godina kažu da imaju profil, iako je minimalna starosna granica, propisana od strane društvenih mreža, obično 13 godina.

Aplikacije su nam tu da nadziremo ljubimce kada odemo na posao i ostavimo ih same u kući ili stanu, kao i da nam pomognu da ih lociramo kada se izgube i "odu svojim poslom".

Neke druge aplikacije nam pomažu da prepoznamo cveće i biljke koje vidimo, a ne znamo kako se zovu, kao i da organizujemo svoje bašte i cvetne vrtove.

U svim tim aplikacijama, dok nam se životi organizuju oko njih, a ne obrnuto, često zaboravimo da sebi postavimo pitanje - šta će nam ostati kada nestane wi-fi signal?

Korišćene reference, linkovi & izvori

Lozinke:

- https://www.cmu.edu/iso/governance/guidelines/password-management.html
- https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf
- https://specopssoft.com/blog/password-length-best-practices/
- http://cups.cs.cmu.edu/soups/2012/proceedings/a7_Shay.pdf
- https://shredcube.com/passphrases-vs-passwords/
- https://haveibeenpwned.com/Passwords
- https://haveibeenpwned.com/
- https://howsecureismypassword.net/
- https://www.pcmag.com/how-to/simple-tricks-to-remember-insanely-secure-passwords

Menadžeri lozinki:

- https://medium.com/@stuartschechter/before-you-use-a-password-manager-9f5949ccf168
- https://www.pcmag.com/picks/the-best-free-password-managers
- https://keepass.info/
- https://www.techradar.com/best/password-manager
- https://medium.com/@stuartschechter/before-you-use-a-password-manager-9f5949ccf168

Softveri & malveri:

- https://www.it-klinika.rs/blog/zasto-je-vazno-azurirati-os-i-softver
- https://www.it-klinika.rs/blog/sta-je-malver-i-kako-se-odbraniti
- https://support.microsoft.com/sr-latn-rs/topic/kako-se-spre%C4%8Davaju-i-uklanjaju-virusi-i-drugi-malver-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5
- https://resursi.sharefoundation.info/wp-content/uploads/2018/10/vodic_osnove_digitalne_bezbednosti_-_preview.pdf

Protokoli komunikacije & zaštita podataka:

- https://pcpress.rs/chrome-uskoro-pocinje-da-daje-prednost-https-protokolu/
- https://smartweb.rs/https-put-ka-vise-poseta-kupaca/
- https://www.it-klinika.rs/blog/sta-je-ssl-i-kako-doprinosi-zdravlju-web-sajta
- https://www.cloudflare.com/learning/ssl/why-is-http-not-secure/
- https://www.youtube.com/watch?v=hExRDVZHhig

Dvofaktorska autentifikacija:

- https://www.merchantfraudjournal.com/two-factor-authentication-work/
- https://authy.com/what-is-2fa/
- https://www.mathema.hr/zasto-je-vazno-koristiti-dvofaktorsku-autentifikaciju-2fa-2219/
- https://searchsecurity.techtarget.com/definition/two-factor-authentication

Pretraživači & personalizovana pretraga:

- https://en.wikipedia.org/wiki/Google_Analytics
- https://en.wikipedia.org/wiki/Filter_bubble
- https://duckduckgo.com/
- https://en.wikipedia.org/wiki/List_of_Google_products

Pregledači & privatnost na Internetu:

- https://pcchip.hr/Internet/kako-se-koristi-tor-web-preglednik-za-anonimno-surfanje/
- https://lab.miletic.net/hr/nastava/materijali/tor-anonimna-komunikacija/
- https://en.wikipedia.org/wiki/Tor_(anonymity_network)
- https://www.torproject.org/download/
- https://core.ac.uk/download/pdf/19790173
- https://kompjuteras.com/adblock-plus-dodatak-namena-upotreba/8.pdf

Privatnost na društvenim mrežama:

- https://www.digitalnimarketing.in.rs/13-popularnih-drustvenih-mreza/
- https://backlinko.com/social-media-users
- https://medik.rs/vesti/idemo-jos-jedan-krug-vreme-provedeno-na-drustvenim-mrezama-ne-utice-na-mentalno-zdravlje
- https://www.statista.com/statistics/617136/digital-population-worldwide/

Geooznačavanje:

- https://www.silkstream.net/blog/2016/08/geotagging-social-media-risks.html
- https://support.google.com/accounts/answer/
- https://africantravelinc.com/sites/default/files/Social%20Media%20Responsiblity%20Card_0.pdf
- https://www.travelpulse.com/news/travel-technology/geotagging-social-posts-are-harmful-to-animals-and-natural-areas.html

ZAHVALNICA

U sastavljanju beleški koje ste pročitale su, samoinicijativno, učestvovale polaznice druge Digitalne feminističke škole koje su tokom proleća 2021. godine učestvovale na radionicama digitalne bezbednosti.

Za uređivanje tekstova, kao i za dizajn i prelom brošure, bila je zadužena **Hristina Cvetinčanin Knežević**, koja je održala pomenute radionice dok je finalnu lekturu uradila **Nađa Bobičić**.

Polaznice koje su istraživale, pisale, lektorisale i za vas spremile tekstove koji sačinjavaju *Radne beleške o digitalnoj bezbednosti* su:

Aleksandra Baša
Aleksandra Ivanović
Anđelija Draško
Dunja Gusić
Irena Karadarević
Magdalena Ilieva
Marija Brajković Marković
Marija Sibinović
Nadija Mustapić
Sandra Knežević
Sanja Lečić
Tamara Kovačević
Višnja Bošković

Sav rad na ovim beleškama je bio u potpunosti volonterski, kako bismo podelile ono što znamo i pozivamo vas da ih, u istom duhu, delite sa svojim prijateljicama & prijateljima, kako bismo na Internetu zajedno bili što bezbednije & bezbedniji!

OAK FOUNDATION

trag FONDACIJA

DFŠ 2021

Program Digitalne feminističke škole se organizuje uz podršku fondacije OAK/Trag.