ONLINE SIGURNOST 101

one world platform

Page intentionaly left blanc

ONLINE SIGURNOST 101

One World Platform
Sarajevo, Bosna i Hercegovina

https://oneworldplatform.net
https://zenskaposla.ba

info@oneworldplatform.net

Autorice: Valida Hromadžić i Tina Lukežić
Grafički dizajn i DTP: Denis Šparavalo Shpary

Priručnik je dio projekta “Jačanje online sigurnosti sigurnih kuća”, koji je fondacija “Platforma Jedan Svijet” (OWP) realizovala u period juli-decembar 2017, uz finansijsku podršku “Asocijacije za Progresivne Komunikacije” (APC).

one world platform

APC

Page intentionally left blanc

Godine 1993. Generalna skupština Ujedinjenih naroda usvojila je Deklaraciju o ukidanju nasilja nad ženama (A / RES / 48/104). Deklaracija definira nasilje nad ženama kao
"bilo koji čin rodno zasnovanog nasilja koji rezultira, ili će vjerovatno rezultirati, fizičkim, seksualnim ili psihološkim povredama ili patnjama žena, uključujući prijetnje takvim djelima, prisilnom ili svojevoljnom lišenju slobode, bilo da se javljaju u javnom ili privatnom životu".

Šta je online nasilje nad ženama?

Kada govorimo o online nasilju nad ženama, odnosno nasilju koje je povezano sa tehnologijom, tj. IKT-om (informaciono-komunikacionim tehnologijama), ono obuhvata akte rodno zasnovanog nasilja koji su počinjeni, podstaknuti ili pogoršani, djelomično ili u potpunosti, upotrebom IKT-a, kao što su telefoni, internet, platforme društvenih mreža i email. Nasilje nad ženama koje je povezano sa tehnologijom je dio istog kontinuuma kao i nasilje nad ženama u fizičkom prostoru (offline).

U fizičkom prostoru, na ulicama i domovima, djevojke i žene se suočavaju sa određenim rizicima. U online prostoru, izložene su onlajn (online) uznemiravanju, sajber uhođenju (cyber stalking), invaziji privatnosti, uz prijetnje ucjenama, viralnim 'videima silovanja', a što je specifično za mlade djevojke, distribuiranje 'videa sex-a' koja prisiljavaju preživjele da ponovo proživljavaju trauma seksualnih napada svaki put kada se objave online, putem mobilnih telefona ili se distribuiraju na druge načine.

Sajberuhođenje/virtuelno uhođenje (cyberstalking) uključuje ali nije ograničeno na:
- Uznemiravanje, ponižavanje i sramoćenje dotične osobe
- Uznemiravanje obitelji, prijatelja i poslodavaca dotične osobe u cilju njenog izoliranja
- Taktike da se zastraši dotična osoba
- Preuzimanje identiteta druge osobe
- Praćenje osobe (npr.korištenje Facebook/Viber obavijesti da bi se saznala lokacija osobe, koristeći softvere za praćenje, aktiviraje GPS-a/lokacija osobe koja se želi pratiti)

Online nasilje nad ženama nije novi vid nasilja, samo je kanal nasilja novi. Nasilje nad ženama koje je povezano sa tehnologijom krši pravo žena na samoodređenje i tjelesni integritet. To uzrokuje psihičku i emocionalnu štetu,

pojačava predrasude, šteti ugledu, uzrokuje ekonomske gubitke i postavlja prepreke za učestvovanje u javnom životu te može dovesti do seksualnog i drugih formi fizičkog nasilja.

IKT imaju niz karakteristika koje ih čine pogodnim alatom za zlostavljanje. Kako se zlostavljanje vrši sa distance, identifikacija i mogućnost da se poduzme mjera protiv zlostavljača/uznemirivača postaje mnogo teža.

Danas svaka osoba samo koristeći mobilni telefon može preuzeti i objavljivati slike i video zapise druge osobe, a te iste može replicirati nebrojeno puta bez ikakvog troška.

U većini slučajeva ljudi ne znaju šta da učine da bi sebe zaštitili od takvih kršenja prava. Telekomunikacione kompanije, internet provajderi i programeri/ke moraju zaštiti korisničku privatnost i sigurnost. Vlade moraju osigurati zakone i politike kao odgovor na ovaj relativno novi oblik nasilja nad ženama.

Kako nefizičko nasilje može biti štetno?

Psihološko nasilje je prepoznato kao vid nasilja i jasno je definisano u okviru međunarodnog prava kao kršenje ljudskog prava. Štetu koju uzrokuje nasilje povezano sa tehnologijom uključuje emocionalnu i psihološku štetu, štetu po reputaciju osobe, fizičku štetu, te invaziju privatnosti, gubitak identiteta, ograničenje kretanja, ceunzuru kao i gubitak imovine. Ove forme nasilja utiču na mogućnost ženske osobe da se slobodno kreće, bez straha od praćenja.

Mapirajući slučajeve online nasilja na "Take Back the Tech!" online map (projekat koji je implementirala "Asocijacija za Progresivne Komunikacije"), evidentno je da su 3 kateogorije žena najizloženije online nasilju:

- Žene u intimnim vezama čiji su partneri postali zlostavljači;
- Žene koje su preživjele fizičke napade — često zlostavljane i silovane od strane intimnih partnera;
- Ženske osobe iz javnog života, odnosno one čiji su javni profili uključeni u javnu komunikaciju (spisateljice, istraživačice, aktivistkinje i umjetnice).

Upotreba tehnologije i nasilje u porodici

Kao i sve forma nasilja nad ženama, i online nasilje vrše osobe koje poznaju preživjelu. Kada se radi o slučajevima nasilje nad ženama koje je povezano sa

tehnologijom a koje se odvija u kontekstu nasilja u porodici, žene su izložene fizičkom premlaćivanju i/ili seksualnom zlostavljanju, praćeno vrijeđanjem, zastrašivanjem ili nasilnim SMS porukama, telefonskim pozivima ili emailovima. U nekim drugim slučajevima, nakon završetka intimne veze, privatne i intimne fotografije, te videa žena bivaju objavljena na internetu u svrhu osvete i zastrašivanja. U nekim slučajevima nasilje počinje online i prenosi se u fizički prostor. Na primjer, ženi se prvobitno prijeti putem mobilog telefona, čin nasilja koji vremenom eskalira do silovanja.

Šta je 'revenge porn'?

'Revenge porn' je uvelike povreda ženine privatnosti. To su slučajevi gdje se privatna i seksualno eksplicitna videa i fotografije javno objave bez jasne saglasnosti i dozvole osobe koja je snimana. Ova videa i fotografije se postavljaju na različite web stranice u svrhu iznuđivanja, ucjene i/ ili ponižavanja. Ovaj termin opisuje čin nasilja i ne treba ga poistovjećivati sa pornografskim sadržajem. U slučajevima 'revenge porn-a' se radi o osveti (najčešće ženama) zbog odbijanja bračne ponude ili prekida veze iz bilo kojeg razloga.

Nasilje nad ženama i društvene mreže

Najčešće forme nasilja nad ženama koje se odvijaju na društvenim mrežama su:

- Kreiranje lažnih profila žena, često da bi bile oklevetane, diskreditovane i s ciljem uništavanja reputacije
- Širenje privatnih i/ili seksualno eksplicitnih fotografija/videa s ciljem nanošenja štete i/ili ucjene
- Stranice, komentari, postovi i slično koji su usmjereni na rodno zasnovanu mržnju (mizoginična nipodaštavanja, prijetnje smrću, prijetnje seksualnim nasiljem itd.)
- Objavljivanje ličnih informacija o ženama koja uključuju imena, adrese, brojeve telefona i email adrese bez saglasnosti žena.

Strategije za zaštitu vaše online privatnosti

Zaštita ličnih podataka na kompjuteru

U kompjutere i telefone pohranjujemo jako mnogo informacija o tome ko smo i šta radimo. Nije na odmet biti svjestan/svjesna o nekoliko stvari koje mogu zaštiti vaše lične podatke na kompjuteru/telefonu koji koristite.

Prvo razmislite šta ili koga štitite i od čega. Odgovori mogu biti u rasponu od slučajnih napada virusa do spywera (u osnovi dosadni programi koji se prikače na vaš kompjuter bez vaše dozvole i prikupljaju informacije s njega), do ljudi koji imaju fizički pristup vašem kompjuteru. U nastavku slijede neki od konkretnih koraka za rješavanje ovakvih, i drugih potencijalnih prijetnji.

Zaštita vaših podataka, identiteta i kompjutera

- Kreirajte gost-korisnički profil na vašem kompjuteru i neka drugi ljudi koriste kompjuter sa tim korisničkim profilom. Na ovaj način druge ljude držite podalje od vaših datoteka i podataka
- Lozinkom zaštitite foldere i dokumente koji sadržavaju osjetljive informacije
- Uvijek budite oprezni kada dajete svoje lične podatke (npr.vaše ime, adresu, broj telefona, itd.) pri korištenju interneta
- Web stranice generalno imaju sporazume o privatnosti ako traže vaše lične informacije. Pročitajte te sporazume i saznajte kako namjeravaju koristiti vaše podatke u slučajevima da ih podijele sa trećom stranom itd.
- Uvijek imajte instaliran pouzdan antivirusni program. Onaj koji redovno ažurira svoje baze da bi mogao da prati najnovije viruse koji inficiraju internet. Podesite vaš kompjuter da na dnevnoj osnovi provjerava vaš kompjuter
- Pobrinite se da anti-virus automatski provjerava dolazeće mailove i preuzimanja (downloads)
- Nikada ne otvarajte privitke emaila (attachments) osim ako ste potpuno sigurni da dokument nije zaražen
- Kada koristite USB drive koji je korišten na drugom kompjuteru, pokrenite anti-virusni program na njemu da se uvjerite da je 'čist'.

Krađa identiteta — phishing

Gdje se kradu vaši lični podaci korisničkih računa?

Jeste li ikada 'izgubili' vaš Yahoo! email račun? Jeste li se ikada pitali kako neko uspije doći do vaših kontakt podataka koji bi trebali biti zaštićeni lozinkom?

Jedna od metoda je poznata kao 'phishing'. To je kada vam se putem lažnih mailova ili instant poruka ili čak putem telefona traži da otkrijete povjerljive informacije poput lozinki ili druge detalje korisničkog računa.

Ponekad takav email može izgledati vrlo uvjerljivo sa zvaničnim logoima i internet adresama ili URL-ovima koji se čine autentičnim, ali u stvari sadrže male razlike koje će vas navesti na interent stranicu krađe identiteta/prevare (phishing website). Na primjer, namjerno pogrešno napisane riječi koje se mogu previdjeti, ili postavljanje teksta sa ispravnom URL adresom, ali stvarno aktivan link vas vodi negdje drugo, itd. Kada se nađete na takvim, lažnim, stranicama, bilo koje detalje da prijavite, prevarant/i ih pohranjuju. Na Yahoo! primjeru, vašem stvarnom prijatelju korisnički račun može biti 'upecan' i onda se njegov ukradeni identitet koristi za kontaktiranje ostalih ljudi iz njegove liste i tako se nastavlja i širi prevarantsko prikupljanje podataka.

- Obično je cilj krađa identiteta usmjerena na finansijski rizik i gubitak, gdje se bankovni podaci nehotice pošalju na lažne stranice i sl. Ali, kroz kršenje ličnih komunikacija i prava na privatnost, 'phishing' također može izazvati veliku štetu društvenim odnosima iz online na offline području i može rezultirati emocionalnim i psihološkim povredama.

Osnovni savjeti za online chat

- Ne koristite opciju "automatsko pamćenje lozinke" (automatically remember your password). Ako koristite ovu opciju, znači da će se svako ko koristi vaš kompjuter moći prijaviti na vašu uslugu za komunikaciju (ili idruštvenu paltformu) koristeći vaše korisničko ime i lozinku
- Ako se odlučite da aktivirate opciju arhiviranja vaših online razgovora, budite sigurni gdje čuvate arhivu na vašem disku, tako da je možete izbrisati ako je potrebno ili je premjestiti na drugi (sigurniji) uređaj za pohranu podataka.

Mobilni telefoni

- Razmislite o tome da lozinkom zaključavate svoj telefon kao način na koji bi svi vaši podaci koji se nalaze u telefonu ostali privatni u slučaju da izgubite telefon ili vam bude ukraden.
- Ako dobivate uznemirujuće poruke, ne brišite ih. One mogu biti važan dokaz ako budete morali pružiti dokumentaciji policiji ili pružatelju telefonskih usluga. Ako primate uznemirujuće telefonske pozive, provjerite da li vaš telefon ima mogućnost snimanja poziva da biste imali digitalan zapis o onome ko vas uznemirava.

Lozinke/šifre

To može biti dosadan posao, ali dobra praksa pravljenja sigurnih lozinki/šifri je od suštinskog značaja za održavanje sigurnih uređaja i podataka. Možete instalirati softver za kreiranje jake lozinke/šifre i sačuvati sve lozinke/šifre u jednu praktičnu i sigurnu bazu podataka.

U ovu svrhu dobar i provjeren alat je KeePass (KeePassX) (https://www.keepassx.org/) koji radi na svim operativnim sistemima. Postoji i varijanta za mobilne telefone Keepass2Android (https://play.google.com/store/apps/details?id=keepass2android.keepass2android&hl=en)

Digitalna sigurnost je potrebna svim osobama koje koriste internet i dijele svoje podatke. Od vitalnog je značaja da pojedinci/ke koji/e dijele svoje podatke online, saštite svoje podatke i identitet. Nekoliko osnovnih savjeta za zaštitu online podataka:

- Kada koristite bilo koju od digitalnih platformi, pobrinite se da u potpunosti razumijete uslove korištenja iste, kako biste razumjeli implikacije stvaranja i dijeljenja sadržaja u prostoru
- Po mogućnosti koristite anonimnu e-mail adresu prilikom kreiranja i postavljanja svog računa ili profila
- Nemojte dijeliti lične podatke u digitalnom prostoru zbog kojih se ne biste osjećali ugodno da se prate ili se pojave u drugim prostorima ukoliko vaš račun ili stranica budu hakovani
- Bilo kakvo uznemiravanje prijavite administratorima/kama stranice i nastavite se zalagati da se nešto povodom toga uradi.

Servisi i njihove postavke

O Gmail postavkama

Kada koristite Google usluge, npr. pretražujete preko Google-a, tražite uputstva preko Google Maps ili gledate video preko You Tube, Google prikuplja podatke a to može uključivati:

- Pojmove koje pretražujete
- Stranice koje posjećujete
- Videa koja gledate
- Oglase na koje klikate
- Vašu lokaciju
- Informacije o uređaju
- IP adresu i podatke kolačića (cookie)

Google i sadržaji koje kreirate

Ako ste prijavljeni sa vašim Google nalogom (računom), Google pohranjuje i štiti ono što ste kreirali koristeći Google-ove usluge (servise). Ovo uključuje:

- Email-ove koje šaljete i primate putem Gmail-a
- Kontakte koje dodajete
- Kalendar
- Fotografije i videa koje 'uploadujete'
- Dokumente, tabele i slajdovi na Drive-u

Kada kreirate Google nalog (račun), Google čuva vaše osnovne podatke koje im date. Ovo može uključivati vaše:

- Ime
- Email adresu i lozinku
- Datum rođenja
- Rod
- Broj telefona
- Državu

U odjeljku "My Account" (myaccount.google.com) možete pronaći alate/postavke gdje možete upravljati svojom privatnošću i informacijama. U Activity Controls možete podešavati koje podatke Google prikuplja o vama, uključujući Search, YouTube i aktivnosti vezane za lokaciju.

U sekciji "Ads Settings", možete podešavati postavke koje kontrolišu reklame koje vam se prikazuju, a koje vam se prikazuju u skladu sa vašim interesima i pojmovima koje ste pretraživali.

Facebook postavke

Upoznajte se sa ličnim postavkama Facebook profila. Kliknite na "▼" u gornjem desnom uglu (pored znaka upitnika).

U odjeljku "Sigurnost i prijava" imate uvid i pregled uređaja preko kojih ste prijavljeni na Facebook. Ako ne prepoznajete neki od izlistanih uređaja, obavezno poduzmite korake da uklonite taj uređaj.

U pododjeljku "Prijava" imate opcije da promjenite lozinku.

U pododjeljku "Setting Up Extra Security" možete da postavite postavke tako da primate upozorenja o nepoznatim prijavama na vaš račun/profil. Provjerite da li vam je ova opcija uključena.

Ovdje vam se također nudi opcija upotrebe dvostruke provjere autentičnosti.

U odjeljku "Privatnost" možete kontrolisati ko može vidjeti vaše buduće objave, na koji način vas drugi mogu pronaći i stupiti u kontakt s vama.

U odjeljku "Blokiranje" upravljate blokiranjem bilo da se radi o osobama/korisnicima, porukama, aplikacijama, događajima i stranicama.

Instagram postavke

Instagram je jedna od lakših aplikacija za korištenje. Kako biste zaštitili svoju privatnost i lične podatke, osnovni korak koji morate da zadovoljite jeste da izaberete opciju privatnog profila. Privatni profil na Instagramu znači da niko ne može pristupiti vašem profilu niti objavljenom sadržaju (što uključuje vaše fotografije i 'storije' odnosno priče koje se brišu nakon 24 sata), osim ako ga niste prihvatili kao svog pratitelja ili pratiteljicu. Naravno, preporučujemo da za svoje pratitelje odobravate samo one osobe koje lično i poznajete. Također, preporučljivo je da kao Instagram ime ne stavite svoje puno ime i prezime, već da smislite neki nadimak. Ukoliko želite da se potpuno zaštitite, poželjno je ne objavljivati sliku sa navedenom lokacijom u trenutku kada se nalazite na toj lokaciji, već par sati poslije kada ste već otišli. Druge lične informacije poput adrese, broja telefona, adrese vašeg posla i slično ne biste trebali otkrivati jav-

no putem objavljenih slika, video zapisa i komentara.

Kada napravite vlastiti Instagram profil, nađite, odmah pored opcije uređivanja profila, i pritisnite okrugli gumb za sve postavke. Između ostalih, pronaći ćete postavke računa, druge po redu, gdje možete odabrati opciju privatnog računa, imati uvid u fotografije drugih korisnika na kojim se vi pojavljujete, uvid u publikacije za koje ste pritisnuli gumb "sviđa mi se" i listu onih Instagram korisnika koje ste odlučili blokirati.

Pretraživanje interneta

Internet i WorldWideWeb nisu isto. Internet je masivna mreža mrêža, mrežna infrastruktura. Ona povezuje milione kompjutera globalno, čineći mrežu u kojoj svaki kompjuter može da komunicira sa drugim kompjuterom, dok god su oba spojena na internet. WorldWideWeb je način pristupanja informacijama putem interneta.

Bilo da pretražujete Internet na privatnom, poslovnom ili tuđem kompjuteru, dobro bi bilo povesti računa o tome koliko je određeni pretraživač siguran, odnosno koliko prikuplja podataka o vama i koliko prati vaše aktivnosti.

Za početak, sigurnost svog pretraživača možete provjeriti putem Panopticklick (https://panopticlick.eff.org/).

Bilo koji pretraživač da koristite, provjerite zadane postavke.

Za Chrome:
> Postavke (Settings) > Prikaži napredne postavke (Show Advanced Settings) > Privatnost (Privacy) > Pošalji zahtjev "Nemoj pratiti" uz promet pregledavanja (Send "Do Not Track" request with your browser traffic).

Za Firefox:
>Alati (Tools) > Opcije (Options) > Privatnost i sigurnost (Privacy & Security) > Zaštita od praćenja (Tracking Protection). U ovom dijelu postavki izaberite opcije za koje smatrate da vama odgovaraju:

- Uvijek (Always)
- Samo u privatnom prozoru (Only in private window)
- Nikada (Never)

Odnosno, u odjeljku Pošalji web stranicama "Nemoj pratiti" signal da ne želite da vas se prati (Send websites a "Do Not Track" signal that you don't want to be tracked), zavisno od verzije.

- Samo kada koristim zaštitu od praćenja (Only when using Tracking Protection)
- Uvijek (Always)

Malveri (malwares) i antivirusi

Malwer je skraćenica od maliciozni softver koji je osmišljen s namjerom da ugrozi kompjuterski sistem (npr. brisanje podataka). Savremeni malveri su tako dizajnirani da prouđu neprimjećeni dok izvode nepoželjne radnje u pozadini sistema (krađa osjetljivih podataka, omogućavanje preuzimanje kontrole nad kompjuterom korisnika sa daljine u svrhu korištenja tog kompjutera za izvršavanje daljih zlonamjernih napada). Malveri iskorištavaju propuste u samim programima/softverima. U suštini, malveri iskorištavaju propuste u korisničkom operativnom sistemu ili programima koje koristi. U nastavku su predstavljeni neki od najčešćih vrsta malvera.

a. Trojanski konj (trojan horse) je fajl koji izgleda kao obični fajl (.jpg, .doc) ali je ustvari program koji sadržava maliciozni kod, odnosno kod koji nanosi štetu. Često se koristi da bi kreirao „stražnja vrata" (backdoor) tako da se počinioc ove maliciozne radnje može infiltrirati u kompjuter, tablet ili telefon (smartphone) i pokrenuti dodatne operacije na daljinu. Većina Trojanaca za cilj ima preuzimanje kontrole nad nečijim kompjuterom, krađu podataka i ubacivanje drugih malicioznih programa na žrtvin kompjuter. Ovakvim radnjama može izazvati različite vrste štete: presretanje zaštićenih podataka, može snimati, odnosno bilježiti kucanje na tastaturi tako da se ukucane šifre mogu koristiti za krađu ličnih informacija, preuzimanje (download) drugih malicioznih programa i pokretanje DoS (Denial-of-service) napada. Trojanci nemaju mogućnost reproduciranja i inficiranja drugih fajlova niti se mogu samo-replicirati. Trojanci moraju biti aktivirani od strane korisnika (vrlo često otvaranjem koruptovanih e-mail privitaka (attachments) ili preuzimanjem (download) fajla, tako da se oni aktiviraju zbog nepažnje korisnika. Neke vrste trojanaca, kao što je prethodno navedeno kreiraju 'back door', drugi opet presreću Skype i druge VOIP (voice over internet protocol) pozive, snima audio ili video razgovore koje dalje šalje napadaču.

b. Virusi su vrsta malicioznih softvera, osmišljeni tako da se šire sa jednog na drugi kompjuter (baš kao virusi gripe recimo), čineći štetu na fajlovima i drugim programima. To su kompjuterski kodovi koji se sami repliciraju

i modifikuju druge legitimne fajlove i programe. Često se nalaze u .exe fajlovima (fajlovima koji se pokreću za instalaciju programa) u cilju ubacivanja koda koji omogućava dalju replikaciju. Upravo je samoumnožavanje karakteristika koja viruse odvaja od drugih malicioznih softvera. Virusi mogu da se nalaze na kompjuteru neko vrijeme, ne čineći nikakvu štetu, sve do onog trenutka dok korisnik ne pokrene ili otvori fajl. Jednom kada je vaš kompjuter inficiran virusom, mogu biti inficirani i drugi kompjuteri koji su na istoj mreži. Također se može širiti tako što kliknete na privitak (attachment) ili ako dijelite USB drajv sa drugim osobama/kompjuterima, tako da ima sposobnost širenja putm USB drajvova, bluetooth-a, bežičnom mrežom, 3G mrežom ili putem lažnih web stranica i linkova. Kao što je spomenuto, cilj mu je krađa lozinki ili podataka, podataka koje ukucavate putem tastature, oštećivanje fajlova, spamovanje vašim email kontakata ili čak preuzimanje kontrole nad vašim kompjuterom. Čak i vaši mobilni uređaji mogu biti infcirani virusom. Ako recimo preuzimate aplikacije koje nisu iz provjerenih izvora, odnosno od provjerenih kreatora. Virusi mogu biti sakriveni u privicima sadržaja koji se dijelje društvenim mrežama poput smiješnih fotografija, čestitki, ili audio i video fajlova.

c. Crvi (worms) su slični virusima. Šire se sa jednog kompjutera na drugi, međutim, crv se može samoreplicirati i proširiti u bezbroj kopija iako nije aktiviran od strane korisnika. Za razliku od virusa, crvu ne treba program za koji bi se 'zakačio' i aktivirao i umnožavao. Jednom kada crv uđe u kompjuterski sistem, obično putem mrežne konekcije ili preuzetog fajla, može se umnožiti i nastaviti širit putem mreže ili internet konekcije dalje inficirajući neadekvatno zaštićene kompjutere. Kako se svaka kopija crva dalje može samoreplicirati, brzina kojom nastavljaju širiti mjrežom je jako velika. Crvi iskorištavaju veliku količinu sistemske memorije ili propusnosti mreže. Crv može biti 'ugrađen' u stranicu te na taj način inficira korisnika, odnosno kompjuter. Ono što crvi između ostalog rade je da brišu fajlove, otvaraju i zatvaraju komunikacijske portove u cilju ometanja prometa.

Antivirus programi

Antivirusi, kao softveri koji pokušavaju da spriječe maliciozne softvere (malvere) da preuzmu vaš uređaj, odnosno pokušavaju da vas zaštite od istih. Virusi su najrasprostranjeniji oblik malvera. Današnji antivirusni programi vas upozoravaju u slučajevima kada pokušate da preuzmete (download) sumnjivi file od vanjskog izvora, i pregledaju fajlove na vašem kompjuteru i uporeduju

sa onim kako bi malver trebao izgledati.

Antivirusni program mogu prepoznati one malvere koji su u osnovi slični primjerima koje su developer antivirusnih programa već analizirali. Neki napredni malveri mogu napasti ili zaobići antivirusni program.

Među preporučenim besplatnim antivirus programima su Avast, Bitdefender i Avira.

Neki od čestih pojmova:

ISP — Internet Service Provider

Pružatelj internetskih usluga je kompanija koja pruža uslugu pristupa i korištenja Interneta svojim korisnicima.

Pružatelji internetskih usluga mogu biti organizirani u različitim formama, kao komercijalna, privatna ili neprofitna organizacija.

IP adresa

IP adresa je jedinstvena adresa kojom se identifikuje uređaj na internetu ili na lokalnoj mreži. Ona omogućava da sistem bude prepoznat od strane drugih sistema preko internet protokola. Postoje dva primarna tipa formata IP adresa koja se koriste danas – IPv4 i IPv6

IP — Internet protokol

Internet protokol obezbjeđuje standardni set pravila za slanje i primanje podataka putem interneta. To omogućava uređajima koji operiraju na različitim platformama da međusobno komuniciraju dok god su povezani na internet.

Internet protokol također obezbjeđuje osnovne instrukcije za prenos 'paketa' između uređaja. Internet protokol ne uspostavlja konekciju i ne definiše upravljanje paketima između uređaja. Ovim aspektima rukovodi "Transmission Control Protocol", koji radi u saradnji sa Internet Protokolom na transferu podataka između sistema na internetu. Zbog toga se konekcije između sistema povezanih internetom, često nazivaju"TCP/IP" konekcije.

Metapodaci (metadata)

Metapodaci su informacije koje se kreiraju u trenutku ostvarivanja telefonskog poziva ili kada kreirate email:

- Brojevi telefona i lokacije pozivatelja i primatelja poziva
- Vrijeme poziva i trajanje poziva
- Serijski brojevi telefona
- Email adrese
- Vrijeme i lokacija na koju je email poslan
- Kontekst naziva emaila/poruke (subject line)

Metapodaci su sadržani i u fotografijama, videima, pdf i word dokumentima i uključuju:

- Vrijeme i datum kada je dokument kreiran
- Korisničko ime osobe koja je kreirala i uredila dokument
- Informacije o uređaju koji je kreirao dokument, fortografiju ili video

Kolačići (Cookies)

'Kolačić' (cookie) je dio informacije u formi veoma malog tekstualnog fajla koji je pohranjen na korisnikovom hard drajvu. Kod nekih pretraživača 'kolačić' je mali fajl, a kod nekih, kao kod Firefoxa, svi 'kolačići' se spremaju u jedan fajl.

Kreiraju ga serveri web stranica (kompjuter koji upravlja web stranicom). Informacije koje 'kolačić' sadrži zadaje server i server ih koristi kada god korisnik posjeti dotični sajt. 'Kolačić' se može posmatrati kao neka vrsta identifikacione karte, koja govori web stranici, kada se korisnik/ca ponovo vratio/la na stranicu.

'Kolačići' često pohranjuju vaše postavke pretraživača, kao što je vaš izbor jezika ili lokacija. Također, 'kolačići' mogu da pohranjuju široki spektar informacija koje uključuju podatke preko kojih korisnikk može biti identifikovan (kao što su ime, kućna adresa, email adresa ili broj telefona).

Svrha kolačića je da ubrza interakciju između korisnika i web stranice i omogućavaju web stranicama da prate navike surfanja korisnika i u skladu s tim pravi profile u marketinške svrhe.

Za upravljanje 'kolačićima' posjetite postavke vašeg pretraživača.
Za Chrome (chrome://settings/content/cookies).
Za Firefox (about:preferences#privacy).
Za Operu (Menu–Settings–Privacy and Security)

Novi anonimni prozor

Chrome (New incognito window)
Novi anonimni prozor sprečava Chrom da sačuva zapis o onome što posjećujete i preuzimate.

Napomena: vi ste i dalje vrlo vidljivi na webu, samo Chrome u ovom slučaju 'ne snima' podatke o onome što posjećujete i preuzimate. Osobe s kojima dijelite kompjuter, u ovom slučaju neće moći pratiti vašu aktivnost putem

pretraživača, ali knjižne oznake (bookmarks) i preuzimanja (downloads) će biti spašeni. Chrome tvrdi da sljedeći podaci neće biti spašeni: vaša istorija pretraživanja, 'kolačići' i podaci sajtova te informacije koje ste unijeli u određena polja odnosno forme. Vaše aktivnosti i dalje mogu biti vidljive web stranicama koje posjećujete, vašem poslodavcu ili školi te vašem pružatelju internet usluga.

Firefox — Novi privatni prozor (New Private Window)
Ova opcija omogućava pretraživanje bez spašavanja podataka o tome koje stranice posjećujete.

Kao i kod Chroma, ova opcija pretraživanja vas ne čini anonimnim, samo sprečava Firefox da sačuva zapis o onome što posjećujete i preuzimate.

Izvori korišteni i prilagođeni za izradu ovog materijala:

https://tacticaltech.org/

https://securityinabox.org/en/

https://www.genderit.org/onlinevaw/faq/

https://www.takebackthetech.net/know-more

https://techterms.com/

https://www.aboutcookies.org/

https://www.eff.org/

https://panopticlick.eff.org/

https://us.norton.com/

https://www.kaspersky.com/

https://myaccount.google.com

https://privacy.google.com

Feministički Principi Interneta 2.0

Preambula Feministički internet cilja ka osnaživanju što više žena i queer osoba — u svoj našoj različitosti — kako bi u potpunosti uživale naša prava, upustile se u igru i tražile zadovoljstvo, i demontirale patrijarhat. To doprinosi integraciji naših različitih realnosti, konteksta i specifika — uključujući uzrast, ne|sposobnost, seksualnost, rodne identitete i izražaje, socio-ekonomske položaje, politička i vjerska uvjerenja, etnička porijekla i rasne oznake. Sljedeći ključni principi ključni su u procesu ostvarivanja feminističkog interneta.

Pristup

1. **Pristup internetu** — Feministički internet cilja da omogući da što više žena i queer osoba uživaju univerzalni, prihvatljiv, jeftin, neuslovljen, otvoreni, punoznačni i ravnopravni pristup internetu.
2. **Pristup informacijama** — Podržavamo i štitimo neograničeni pristup informacijama koje su relevantne za žene i queer osobe, a naročito informacije o spolnom i reproduktivnom zdravlju i pravima, zadovoljstvu, bezbjednom abortusu, pristupu pravdi i LGBTIQ pitanjima. To uključuje različitost po pitanju jezika, sposobnosti, interesa i konteksta.
3. **Korištenje tehnologije** — Žene i queer osobe imaju pravo da kodiraju, osmišljavaju, prilagođavaju i koriste, na održiv način, IKT-je i da preuzmu kontrolu nad tehnologijom kao platformom za kreativnost i izražavanje, kako i da ospore i izazovu kulturu seksizma i diskriminacije u svim prostorima.

Pokreti i javno učešće

4. **Otpor** — Internet je prostor u kojem se o društvenim normama pregovara, u kojima se one ostvaruju i nameću, često kao nastavak drugih prostora koje su oblikovali patrijarhat i heteronormativnost. Naša borba za feministički internet jeste ona borba koja se nastavlja na naš otpor u drugim prostorima, javnim, privatnim i onim između.
5. **Transformativni prostor** — Internet je transformativni politički prostor. On pomaže nastajanje novih formi građanstva koje omogućavaju jedinkama da traže, konstruiraju i izraze svojstva, rodove i spolnosti. To uključuje povezivanje preko granica, zahtijevanje odgovornosti i transparentnosti, i stvaranje mogućnosti za održivo stvaranje feminističkih pokreta.
6. **Odlučivanje u upravljanju internetom** — Vjerujemo u osporavanje i izazivanje patrijarhalnih prostora i procesa koji kontroliraju upravljanje internetom, kako i u postavljanje što više feministica i queer osoba u forume na kojima se donose odluke. Želimo da demokratiziramo usvajanje

politika koje utiču na internet, kao i difuzno vlasništvo i moć u globalnim i lokalnim mrežama.

Ekonomija

7. **Alternativne ekonomije** — Posvjećene smo propitivanju kapitalističke logike koja gura tehnologiju ka daljoj privatizaciji, logici profita i korporativne kontrole. Radimo na stvaranju alternativnim formi ekonomske moći koje su zasnovane na načelima suradnje, solidarnosti, zajedničke svojine, ekološke održivosti, i otvorenosti.
8. **Slobodni i otvoreni izvorni kôd** — Posvjećene smo stvaranju tehnologija i eksperimentiranju sa njima, uključujući i digitalnu sigurnost i bezbjednost, i korištenju, alatki, platformi i softvera sa otvorenim i slobodnim izvornim kodom (FLOSS). Promocija, širenje i razmjena i dijeljenje znanja o korištenju FLOSS-a centralni je element naše prakse.

Izražavanje

9. **Jačanje glasnosti feminističkog diskursa** — Tražimo za sebe moć interneta da pojača glasnost ženskih narativa i životnih realnosti. Postoji potreba za odupiranje državi, religioznoj desnici, i drugim ekstremističkim snagama koje monopoliziraju diskurs o moralu i moralnosti, a istovremeno utišavaju feminističke glasove i progone zaštitnice/ke ženskih ljudskih prava.
10. **Sloboda izražavanja** — Branimo pravo na spolno izražavanje kao pitanje slobode izražavanja ne manje važnog od političkog ili vjerskog izražavanja. Žestoko se protivimo naporima državnih i ne-državnih aktera da kontroliraju, upražnjavaju nadzor, reguliraju i ograniče feminističko I queer izražavanje na internetu korištenjem tehnologije, zakonodavstva ili nasilja. To smatramo dijelom šireg političkog projekta moralne policije, cenzure i hijerarhizacije građanstva i prava.
11. **Pornografija i 'štetni sadržaji'** — Razumijemo da je pitanje online pornografije pitanje djelovanja, saglasnosti, moći i rada. Odbacujemo jednostavne kauzalne veze između korištenja pornografskih sadržaja i nasilja nad ženama. Takođe odbacujemo krovni termin 'štetnog sadržaja' kada se odnosi na izražavanje ženske i transrodne spolnosti. Podržavamo osvajanje kontrole nad alternativnim erotskim sadržajima i stvaranje istih na način koji se suprotstavlja dominantnom patrijarhalnom pogledu i koji postavlja želje žena i queer osoba u centar interesa.

Utjelovljenje

12. **Saglasnost** — Ukazujemo na potrebu za izgradnjom etike i politike saglasnosti u kulturi, dizajnu, politikama i uslovima za pružanje usluga na internet platformama. Ženska djelatnost nalazi se u njihovoj sposobnosti da nose informirane odluke o tome koje će aspekte svojih javnih ili privatnih života podjeliti na internetu.
13. **Privatnost i podaci** — Podržavamo pravo na privatnost i na punu kontrolu nad osobnim podacima i informacijama na internetu na svim nivoima. Odbacujemo praksu država i privatnih kompanija da koriste podatke sa ciljem ostvarivanja profita i manipulacijom ponašanja na internetu. Praćenje i nadzor su alatke koje je patrijarhat kroz historiju koristio za uspostavljanje kontrole nad ženskim tijelima, govorom i aktivizmom. Podjednaku pažnju posvjećujemo praksama nadzora i praćenja koje sprovode individualne osobe, privatni sektor, državni i ne-državni akteri.
14. **Djeca i mladi** — Tražimo da se glasovi i iskustva mladih uključe u nošenje odluka o sigurnosti i bezbjednosti na internetu i u promociji njihove sigurnosti, privatnosti i pristupa informacijama. Prihvatamo pravo djece na zdravi emocionalni i spolni razvoj, koji uključuje i pravo na privatnost i pristup pozitivnim informacijama o seksu, rodu i spolnosti u ključnim periodima njihovih života.
15. **Anonimnost** — Branimo pravo na anonimnosti i odbacujemo sve zahtjeve za ograničavanje anonimnosti na internetu. Anonimnost nam omogućava slobodu izražavanja na internet, naročito kada se radi o rušenju tabua spolnosti i heteronormativnosti, eksperimentiranju sa rodnim identitetima i omogućavanju sigurnosti za žene i queer osobe izložene diskriminaciji.
16. **Memorija** — Imamo pravo na upražnjavanje i zadržavanje kontrole nad vlastitim osobnim historijama i memoriji na internetu. To uključuje i mogućnost pristupa svim našim osobnim podacima i informacijama na internetu, kao i mogućnost kontrole nad tim podacima, uključujući i znanje ko im može pristupiti i pod kojim uslovima, kao i mogućnost da ih zauvijek izbrišemo.
17. **Online nasilje** — Tražimo od svih internet stakeholdera, uključujući korisnike, nositelje politika i privatni sektor, da obrate pažnju na pitanje uznemiravanja na internetu i nasilja vezanog za tehnologiju. Napadi, prijetnje, zastrašivanje i nadziranje sa kojima se suočavaju žene i queer osobe su stvarni, štetni i alarmantni, i dio su šireg pitanja rodnog nasilja. Naša je kolektivna odgovornost da ih adresiram i eliminiramo zauvijek.

Sadržaj