BEZBJEDNOST NA INTERNETU U DOBA PANDEMIJE

telenor

DIGITALIZUJ.ME

unicef
za svako dijete

SADRŽAJ

Ova publikacija je nastala u okviru projekta „Bezbjednost na internetu pandemije COVID-a-19", koji realizuje Digitalizuj.Me, uz podršku UNICEF-a i Telenora. Njen sadržaj je isključiva odgovornost organizacije Digitalizuj.Me i ne odražava nužno stavove UNICEF-a niti Telenora.

I. Bezbjednost na internetu u doba pandemije COVID-a-19

Čudna neka godina, priznaćete. Pandemija COVID-a-19, koju ni najmaštovitiji među nama nisu mogli dosanjati, uzburkala je planetu. Eh, da nam je moglo biti da imamo neki naš „Enterprajz" i neprocjenjivog kapetana Žan-Luk Pikarda, koji bi nas za tren izbavio iz nevolje. Ovako, bili smo prinuđeni da se zatvorimo u svoje domove i da spas tražimo u nekom ljepšem imaginarnom univerzumu (kao što je Star Trek za neke od nas).

Totalno zatvaranje, ipak, nije svima teško palo. Iako nam je ograničena jedna od osnovnih ljudskih sloboda, sloboda kretanja, imali smo čitav jedan onlajn univerzum na raspolaganju. Nije isto, saglasni smo, ali čisto sumnjamo da bi iko od nas karantinske dane preživio da nas je ova pošast zadesila u vremenu kad je internet bio misaona imenica.

Bili smo prinuđeni da većinu aktivnosti, što radnih što zabavnih, obavimo onlajn. S obzirom na raznorazne pritiske, rokove i sveopštu paniku izazvanu najnovijom svjetskom nepoznanicom, dosta smo se dobro snašli. Dobro, ali ne i savršeno. Krajnje je vrijeme da priznamo, i drugima i sebi, da nam nije potrebna nova pandemija, niti bilo kakva viša sila, kako bismo pokupili sva potrebna znanja i postali savjesni digitalni građani.

Iz ovakvog razmišljanja rodila se ideja o nizu blog-postova, sklopljeniih u elektronsku knjigu (e-book), kojom ćemo nastojati da pokrijemo neke od najvažnijih aspekata bezbjednosti i ponašanja na internetu (u vanrednim, ali i u redovnim situacijama). Ukoliko ste spremni za nova znanja, ali i za razbijanje pokoje predrasude, hajde da počnemo zajedno. Ili, što bi Pikard rekao: „Engage!"

Autori

- Anja Drobnjak
- Danijela Knežević
- Jevrosima Pejović
- Milutin Pavićević
- Nataša Đukanović
- Sanja Gardašević

II. Zašto je važno kako se ponašamo na internetu?

Da li ste ikada formirali mišljenje o potpuno nepoznatoj osobi samo na osnovu profila na društvenim mrežama? Sasvim je OK ako je odgovor na postavljeno pitanje potvrdan, jer to maltene svi radimo, svjesno ili ne. Svaki status koji objavite na Fejsbuku ili Tviteru, svaka fotografija, video ili muzički zapis koji podijelite čine djelić slagalice koja predstavlja vašu onlajn reputaciju. Onlajn reputacija. Zvuči pomalo zastrašujuće, zar ne? Ali ne brinite, daleko od toga da je nesavladiva, pogotovo uz moćno oružje kao što je znanje. Hajde da zajedno napravimo tri značajna koraka koja će pomoći da naš onlajn identitet predstavimo na najbolji način, jedinstveno i izuzetno, kakvi uostalom (i bez lažne skromnosti) i jesmo.

1. KORAK: Digitalna pismenost 101

Savremena pismenost, pored funkcionalne, obuhvata i digitalnu pismenost. Digitalna pismenost, a posebno digitalna inteligencija, nisu odlično snalaženje u Ekselu, posljednji preživjeli u Fortnajt betl rojalu, mikelanđelovsko umijeće u kreiranju Instagram storija, ili pak vještina spravljanja TikTok videa na kojoj bi vam i Sorentino pozavidio.

Iako je sve navedene vještine lijepo (a neke i neophodno) znati, ovdje ćemo se fokusirati na pitanje zašto je važno biti odgovoran digitalni građanin. Drugim riječima, kako voditi računa o otisku koji vaše digitalno stopalo ostavlja po raznim oblastima onlajn svijeta.

Sve što „uradite" na internetu ostaje na internetu. Zauvijek. To što koristite nik, nadimak ili alijas na Instagramu, Snapčetu ili nekoj drugoj društvenoj mreži nema nikakvu šansu protiv tehnologija za prepoznavanje lica koje koriste pretraživači i koje iz dana u dan napreduju. **Dugme „delete" ne funkcioniše na način na koji bismo željeli.** Iako smo nešto obrisali (nema ga više na tajmlajnu, ne postoji), ne znači da je zaista nestalo. Ali kako?

Niste jedini stanovnik digitalne planete. U moru opcija poput „share" i „screenshot", nikada ne možete biti sigurni da je nešto nestalo. Nažalost, ne postoji crna rupa, spremna da usisa svaki status zbog koga ste se pokajali, sve ne baš reprezentativne fotografije iz provoda, svaki zapis koji je preuranjenim klikom završio u digitalnoj sferi. No prije nego što počnete da očajavate, sjetite se da za sve to postoji krajnje jednostavno rješenje. **Dva puta razmislite prije svake objave.** Zapitajte se da li je to nešto što biste voljeli da vide vaši nastavnici, profesori, rodbina (onaj dio koji nije blokiran). I ne samo oni. Čudesni su digitalni putevi, te dobar dio vašeg sadržaja može lako doći do osobe koja će sjutra birati kandidate za stipendiju za koju ste konkurisali, do budućeg poslodavca, ali - i ništa manje bitno - do osobe koja vam se dopada. Tako da, koliko god naivno zvučalo, nije zgoreg da dobro razmislite o sadržaju koji ćete podijeliti sa žiteljima interneta. Ne kaže se badava „dvaput mjeri, jednom sijeci".

2. KORAK: Svjesno i savjesno građenje ličnog brenda

Vjerovali ili ne, svako od nas ima lični brend, kako u oflajn, tako i u onlajn svijetu. Štaviše, te dvije persone, fizička i digitalna, sve se više preklapaju. Razmislite: koliko puta ste se iznenadili (negativno ili pozitivno) kad ste lično upoznali nekog koga ste prethodno poznavali samo preko društvenih mreža (bilo da je u pitanju fizički izgled, ili pak interesovanja i koeficijent zanimljivosti te osobe)?

Sve što radite „priča" umjesto vas i za vas. Isto važi i za onlajn svijet. Svaka objava je vaš glas na društvenim mrežama, bilo da je u pitanju omiljena pjesma (formiramo mišljenje o vašem muzičkom ukusu), film koji vas je oborio s nogu (formiramo mišljenje o vašem filmskom ukusu), video koji vas je nasmijao (ocjena stepena duhovitosti), knjiga koju ste nedavno pročitali (crvena lampica za knjigofile među nama), ili pak nešto ozbiljnije, poput mišljenja o sveprisutnoj pandemiji virusa, ekonomskoj situaciji, religiji, aktuelnim dešavanjima u svijetu... Preko sadržaja koji dijelite ljudi formiraju sliku o vama. Jako je bitno da se ta slika ne razlikuje (ili makar ne u ogromnoj mjeri) od osobe kakva ste u životu, oflajn. **Lični brend mora biti konzistentan uvijek i svuda, jer on jeste ono što ste vi. Dok u opipljivom svijetu taj brend gradite svojim djelima i riječima, u digitalnom svijetu on predstavlja ideju koju neko ima o vama na osnovu sadržaja koje plasirate na svom parčetu interneta.**

Anonimnost i plašt nevidljivosti, kao elementi svake onlajn komunikacije, omogućavaju nam da kreiramo digitalnu personu po sopstvenoj mjeri, bez onog poznatog pritiska koji obično prati društvene interakcije licem u lice. To nas ohrabruje da na internetu kažemo i prikažemo i više nego što bismo inače. Skriveni iza ekrana, osjećamo se znatno sigurnije i ušuškanije. Greška je u tome što često mislimo da ništa što kažemo tamo negdje na internetu ne može uticati na naš realni život. I te kako može i uvijek se vrati kao bumerang. Stoga, **radite na sebi kako biste se unaprijedili, a digitalni prostor iskoristite da predstavite sebe. Da, u najboljem svijetlu - ne, lažno i isfolirano.**

3. KORAK: Digitalni otisak i kako da „radi" u vašu korist

I pored važnosti onlajn reputacije, činjenica je da većina ljudi ne razmišlja pretjerano o njoj, niti o svim digitalnim tragovima koje ostavlja u sajber prostoru. **Profili na društvenim mrežama postali su moderne verzije ličnih dnevnika, iz kojih možemo da saznamo šta neko voli, koju muziku sluša, gdje je juče ručao (a i šta je imao za ručak), gdje se trenutno nalazi.** I nije da nismo u stanju da neke misli, događaje ili situacije zadržimo za sebe, već će prije biti da ne želimo. To je u redu, dok god postoji mjera. A evo i zašto.

Bezbjednost, bezbjednost, bezbjednost! Dijeljenje velike količine informacija o vašem ličnom životu ne samo da dovodi u pitanje ličnu reputaciju, već može već može biti i opasno, pogotovo za djecu i adolescente. Imajte na umu da digitalni trag ne ostavlja samo nešto što objavite na društvenim mrežama. **Svaki klik, svaka interakcija, pretraga, skinuta aplikacija, sve ostavlja trag i pomaže da dio vaših ličnih informacija dođe do određene baze podataka.**

UNICEF je početkom 2018. godine, u okviru kampanje „Growing up online", predstavio video koji se fokusira na mlade i njihov digitalni otisak. Cilj videa bio je da prikaže koliko podataka i informacija mladi i adolescenti dijele, a da toga nisu ni svjesni. Posebno je interesantan dio koji jasno oslikava neugodnost koju akteri videa ispoljavaju kad se na pres-konferenciji od njih traži da opišu svoj dan, svoje hobije, planove i slično. Ne žele da podijele lične informacije pred gomilom stranaca u realnom svijetu, iako to svakodnevno rade na internetu, gotovo bez razmišljanja. A razlika između ova dva načina dijeljenja zapravo i ne postoji, zar ne?

Šta sve ovo znači kad je u pitanju vaš digitalni otisak? Kao što smo već ustanovili, ne ostavlja trag samo ono što sami podijelite. Takođe, digitalni svijet ima moć da vaše objave prenese do mnogo većeg spektra ljudi nego što se vama u datom trenutku čini. Zbog toga je važno da shvatite i prihvatite da digitalni trag, premda nije opipljiv, zaista postoji. Provjeravajte sve informacije koje pronađete onlajn, kako o drugima tako i o sebi. Razmislite prije nego što nešto podijelite i budite sigurni da sadržaj koji plasirate (ili koji drugi plasiraju, a koji uključuje i vas) nije nešto što vam može nanijeti štetu, bilo danas, bilo za godinu dana. Vodite računa i o privatnosti - razmislite o tome ko sve može vidjeti sadržaj koji dijelite. Kontrola digitalnog otiska (onoliko koliko je moguće upravljati njime) je takođe je značajna. Naravno, mnogo je lakše upravljati sadržajem koji vi plasirate nego onim koji dijeli neko drugi, ali možete, s vremena na vrijeme, izdvojiti par sati da „prečistite" profile na društvenim mrežama, uklonite ili sakrijete sadržaj koji vam se s trenutne vremenske distance ne dopada. Tačno je, rekli smo da dugme „delete" ne čini magiju, ali to ne znači da neće poslužiti kao efikasno sredstvo za čišćenje. Dodatno, obratite pažnju na Politiku privatnosti prilikom aktivacije uređaja i digitalnih usluga koje koristite. Znamo, dosadno je i dugačko, ali šta je dosada spram dijeljenja vaše lokacije, ličnih informacija i istorije pretraživanja potpunim strancima.

Onlajn reputacija i lični brend predstavljaju vašu ličnu kartu na internetu. Ona treba da komunicira autentičnost i vrijednost na način i kroz sadržaj koji vama odgovara, tj. koji vas prezentuje na najbolji način. Kad smo već kod komunikacije, da li ste se ikada našli u *nebranom grožđu* jer je vaša poruka protumačena na pogrešan način?

Komunikacija je važan alat koji svakodnevno koristimo. U vrijeme pandemije COVID-a-19, bili smo prinuđeni da veći dio komunikacije obavljamo onlajn, više nego ikada ranije. Stoga, neće biti zgoreg da naučimo sljedeće:

III. Šta je to što komunikaciju oflajn i onlajn čini toliko različitom?

Da li se iznenadite kad saznate da su vas ljudi pogrešno razumjeli? Izgovarate li često rečenicu: „Nisam ja to tako mislio/mislila"? Obraćate li pažnju na govor tijela onih s kojima komunicirate? Razmišljate li o stavovima svojih sagovornika i zanima li vas njihov ugao posmatranja? Razmišljate li koji kanal komunikacije treba da izaberete kad želite nekome nešto da saopštite?

Komunikacija je jedna od najvažnijih životnih vještina, a vještine se stiču uz mnogo truda. Ne možemo postati vješti komunikatori preko noći. Ipak, ukoliko želimo da maksimalno iskoristimo prilike na koje tokom života nailazimo, neophodno je da se upoznamo s elementima komunikacionog procesa i steknemo vještine kvalitetnog komuniciranja.

Neke od komunikacionih vještina koje nam mogu mnogo pomoći su: pažljivo slušanje, praćenje neverbalne komunikacije, sposobnost kontrole komunikacijskog šuma, sposobnost kontrole stresa u kriznim situacijama, prepoznavanje i razumijevanje vlastitih osjećanja i osjećanja osoba s kojima komuniciramo. Usvajanjem komunikacionih vještina učimo kako da svoje ideje saopštimo jasnije i efikasnije, ali i kako da bolje razumijemo informacije koje se saopštavaju nama.

Komunikacija je proces

Zašto je važno da poznajemo i razumijemo sve faze komunikacionog procesa?

- Da bi nam bilo jasno koja je naša uloga u njemu.
- Da bismo prepoznali šta treba da uradimo kako bi komunikacija bila uspješna.
- Da bismo mogli da predvidimo određene probleme i pronađemo rješenje prije nego što se oni dogode

Najčešći uzrok problema u komunikaciji, ili komunikacijskog klinča, kako ga često nazivamo, jeste nepoznavanje komunikacionog procesa, odnosno nedostatak svijesti o elementima tog procesa. Najčešće mislimo da tokom komunikacije mi pričamo, druga osoba nas sluša — i to je to.

Komunikacioni proces teče ovako: mi nekome nešto kažemo, tj. šaljemo **PORUKU**. Dok tu poruku izgovara-

mo, mi je „pakujemo", tj. **KODIRAMO**, u skladu s našim stavovima, mišljenjima, percepcijom, znanjem, obrazovanjem, raspoloženjem... Ta poruka putuje putem određenog medija (kroz prostoriju, imejlom, putem neke aplikacije, programa...) i stiže do onoga kome je namijenjena. Na drugoj strani naš sagovornik, tj. **PRIMALAC**, tu poruku „raspakuje", tj. **DEKODIRA** i tek nakon toga poruka stiže na svoje odredište. Nakon prijema poruke, sagovornik nam daje odgovor, komentar, stav, tj. šalje **POVRATNU INFORMACIJU** (*feedback*), koja nam otkriva da li je komunikacija uspješna ili ne.

Šta je komunikacioni šum?

Čitav proces „putovanja" poruke prati ŠUM. Komunikacijski šum može biti **psihološki, semantički i mehanički.**

Najčešći oblici **psihološkog šuma** su:

- **filtriranje** (čujemo samo ono što nama odgovara, poruku tumačimo u skladu sa svojim stavovima, vrijednostima, kulturnim preferencijama),
- **percepcija** (proces primanja i selekcije informacija iz okoline putem čula) i
- **emotivno uplitanje** (kakva osjećanja gajimo prema sagovorniku).

Semantički šum odnosi se na način izražavanja. Na nas značajno može uticati vještina izražavanja našeg sagovornika.

Mehanički šum obuhvata sve forme buke iz neposrednog okruženja (vika, šuštanje, prolazak drugih osoba, gužva, saobraćaj, muzika...)

Uspješni komunikatori su tokom komuniciranja uvijek svjesni postojanja šuma i s njim usklađuju svoju komunikaciju.

Zašto je važno da dobijemo povratnu informaciju (*feedback*)?

Osim „borbe" sa šumom, uspješni komunikatori se tokom komuniciranja trude i da dobiju povratnu informaciju. Povratne informacije su nam neophodne jer bez njih ne možemo biti sigurni da su oni koji nas slušaju razumjeli našu poruku na pravi način. Nekad su povratne informacije usmene, a nekad imaju drugačiji oblik.

Povratne informacije koje nam otkriva govor tijela vjerovatno nam mogu najviše pomoći da saznamo da li je naša komunikacija bila efikasna. Razlog je u tome što se govor tijela ne može sakriti, niti odglumiti. Čak ni najvještiji glumci nemaju sposobnost apsolutne kontrole nad govorom tijela. Posmatrajući izraze lica, gestikulaciju i položaj tijela osoba s kojima komuniciramo, možemo zapaziti:

- nivo samopouzdanja;
- defanzivnost;
- slaganje;
- razumijevanje (ili nerazumijevanje);
- zainteresovanost;
- nivo angažovanosti/uticaja poruke;
- iskrenost (ili neiskrenost).

Kao govorniku, razumijevanje govora tijela vašeg slušaoca daje vam mogućnost da svoju **poruku prilagodite i učinite je razumljivijom, dopadljivijom ili interesantnijom.** Kao slušaocu, govor tijela može vam reći više o tome šta govornik saopštava. Zato kažemo da je govor tijela kao povratna informacija PRILIKA.

Naknadno možete postaviti pitanja kako biste bili sigurni da ste zaista razumjeli jedno drugo. Bilo da ste u ulozi govornika ili slušaoca, uz dobro poznavanje govora tijela lakše ćete izbjeći nesporazume.

Pakovanje poruke – kako se kreira poruka?

Kada imamo namjeru da nešto saopštimo, veoma je važno da odlučimo na koji ćemo način to reći. Vješti komunikatori praktikuju KISS princip (*Keep It Simple and Straightforward*).

Neka poruka bude jednostavna i direktna. Manje je često više, a kvalitetna komunikacija treba da bude i efikasna i efektna. Da bismo to postigli, moramo voditi računa ne samo o tome šta ćemo reći, već i o tome **kako će primalac to razumjeti.**

Često se fokusiramo na poruku koju želimo da pošaljemo i na način na koji ćemo je poslati. Ako poruku pošaljemo bez razmišljanja o tome kakva je perspektiva primaoca, velika je mogućnost da će dio te poruke biti izgubljen.

Da biste efikasnije komunicirali, potrebno je da:

- razumijete ono što zaista treba i želite da kažete;
- predvidite reakciju primaoca poruke;
- izaberite riječi i govor tijela koji će osobi koja vas sluša dozvoliti da zaista čuje ono što saopštavate.

Kako biramo kanal komunikacije?

Osim kodiranja (pakovanja) poruke, potrebno je i da izaberemo najbolji kanal komunikacije za njeno slanje.

Imejl je praktičan komunikacioni kanal za slanje jednostavnih uputstava. Ipak, ako želite da nekome pošaljete kompleksniju poruku, imejl poruka će vjerovatno inicirati dodatna pitanja, pa bi najbolje bilo da organizujete sastanak s tom osobom.

Ako ono što želite da saopštite ima bilo kakav negativan emocionalni kontekst, držite se podalje od imejla i drugih vidova pisane komunikacije! U takvim situacijama, postarajte se da komunicirate lično ili putem video-poziva. Tako ćete moći da ocijenite kakav uticaj vaše riječi imaju na osobu kojoj su upućene i imati priliku da ih prilagodite ili ispravite.

O čemu treba voditi računa prilikom odabira najboljeg načina za slanje poruke?

- O osjetljivosti i emocionalnom sadržaju teme.
- Koliko je jednostavno saopštiti detalje poruke?
- Kakve su preferencije slušaoca?
- O vremenskim ograničenjima.
- O potrebi za postavljanjem pitanja i odgovaranjem na pitanja.

U čemu se razlikuju onlajn i oflajn komunikacija?

Nekada je razlika između komunikacije uživo i komunikacije u digitalnom svijetu bila velika i tačno se znalo kakva se komunikacija vodi licem u lice, a kakva se može odvijati putem digitalnih platformi. Kako tehnologija napreduje, tako ta razlika biva sve manja, pa možemo reći da razvoj digitalnih tehnologija, kad je riječ o komunikaciji, ide u pravcu potpunog eliminisanja te razlike. Sada imamo sve kvalitetnije provajdere video-poziva, sve bolja grafička rješenja emotikona, gifova, stikera i raznoraznih „dodataka" čiji je zadatak da dočaraju neverbalnu komunikaciju, odnosno nadomjeste govor tijela, koji u digitalnoj komunikaciji izostaje, a veoma je važan činilac komunikacije (naročito kao oblik povratne informacije).

Globalne vanredne situacije, poput aktuelne pandemije koronavirusa, pokazale su i onim najtvrdokornijim protivnicima digitalne komunikacije koliko je važno raditi na sebi i usvajati nove vještine. Sve je manje onih koji se opiru digitalnim komunikacijama — upravo zahvaljujući njima ljudi i dalje mogu kvalitetno poslovno da funkcionišu i zarađuju za život.

Onlajn komunikacioni proces se, dakle, sve manje razlikuje od oflajn komunikacionog procesa.

Ipak, postoji nešto što je primjetno u svijetu onlajn komuniciranja i što onlajn komunikaciju čini drugačijom od oflajn komunikacije. Riječ je o digitalnoj anonimnosti, odnosno psihološkom efektu koji digitalna anonimnost proizvodi — stručnjaci za digitalnu bezbjednost bi vjerovatno rekli o efektu prividne anonimnosti budući da apsolutna digitalna anonimnost ne postoji, ili je bar nedostižna prosječnim internet korisnicima.

Veoma je jednostavno napraviti lažni profil na društvenim mrežama i komunicirati kao „alter ego", ili pak komentarisati na platformama na kojima nikada ne bismo poželjeli da se nađe naše pravo ime. U onlajn svijetu se pod lažnim imenima komunicira po zadatku, s određenim ciljem, namjerom, s upitnom autentičnošću, lažnom samouvjerenošću... Oni koji praktikuju takav vid komunikacije ne plaše se posljedica dijelom zato što norme koje regulišu onlajn komunikaciju postoje, ali se njihovo nepoštovanje najčešće ne sankcioniše. Sve to dovodi do stvaranja lošeg digitalnog okruženja.

Upitajmo se koliko imamo razumijevanja za objave drugih ljudi. Da li odmah komentarišemo, ili prije kucanja komentara razmislimo o okolnostima zbog kojih je ta objava baš takva? Jesmo li brži u pozitivnom ili negativnom komentarisanju? Da li neka rasprava u digitalnom svijetu kod nas izaziva nemir i ljutnju? Razmišljamo li o tome kako će ljudi koji nas ne poznaju protumačiti ono što napišemo?

U digitalnom svijetu ne komuniciramo s mašinama, nego s ljudima. I u onlajn i u oflajn svijetu treba se voditi citatom poznatog ruskog književnika i filozofa Lava Tolstoja: „Prestani da govoriš onog trenutka kad primijetiš da se sam uzrujavaš ili da to čini onaj kome govoriš." No, kako se ne pridržavaju svi ovog zlatnog pravila, onlajn komunikacija sve češće poprima obrise digitalnog nasilja, tzv. sajberbulinga.

IV. Sajberbuling - pakao savremenog tinejdžera

Godina je 1998. Petaci čekaju da počne čas istorije. Odjednom se čuje komešanje, škripa klupa i grupno, sinhronizovano: „Uuuuu!" U ćošku, pored korpe za otpatke, nova djevojčica u odjeljenju tuče Veljka, budućeg fudbalskog reprezentativca! Ovaj događaj se prepričava na svakom organizovanom i spontanom okupljanju uz nove opaske i detalje. Glavni akteri obično ublažavaju i trude se da priču drže u granicama realnog. Veljku ni danas, dvadesetak godina kasnije, nije prijatno, ali stojički podnosi šale. Sportista kojeg je pretukla djevojčica, pa to je horor film svakog tinejdžera! Ne može se zamisliti gori scenario... ili ipak može? Godina je 2020. Petaci čekaju da počne čas istorije. Na jednom komešanje, škripa klupa... Uz grupno, sinhronizovano: „Uuuuu!", vadi se minimum 20 telefona i bilježi trenutak najveće sramote mlade nade crnogorskog fudbala.

Legenda o batinama u video-formi na raznim platformama, putuje znatno brže do ušiju drugih odjeljenja, zbornice, drugova iz kluba, roditelja... svih! Nakon par dana kreću mimovi... Jednom riječju, pakao!

Ukoliko imate nalog barem na jednoj društvenoj mreži, poznat vam je ovaj scenario, zar ne? Svađa drugara, kad se pojavi onlajn, izgubi potencijal da bude glavna šala u društvu i prerasta u sajberbuling (*cyberbullyng*).

Sajberbuling, zlostavljanje na internetu ili digitalno nasilje, jeste uznemiravanje, ismijavanje, zastrašivanje i emocionalno povređivanje jedne osobe ili grupe osoba na društvenim mrežama. Ovaj vid nasilja najčešće se ispoljava postavljanjem neprimjerenih i uvredljivih poruka i fotografija na društvenim mrežama, ili slanjem poruka na različite adrese.

Sa sajberbulingom se vrlo teško nositi – skoro ga je nemoguće kontrolisati, što znači da osoba može biti neprestalno izložena takvom nasilju, 24 sata, sedam dana u nedjelji. Nasilnici u virtuelnom svijetu često nemaju imena niti lica koja možemo zapamtiti kako bismo ih mogli izbjeći, prijaviti nastavniku/nastavnici ili roditeljima, koji bi kasnije porazgovarali s njegovim/njenim roditeljima.

Kako izgleda sajberbuling?

Danas, više nego ikada ranije, veliki dio vremena provodimo onlajn. Zato je vrlo važno prepoznati kad nečije ponašanje u onlajn svijetu prestaje da bude OK. Zlostavljanje na internetu ispoljava se u različitim formama. To može biti:

- *Postavljanje uvredljivih poruka, imejlova ili komentara na veb-platformama.* Posebno obratite pažnju kad vam neko uputi neku takvu poruku „kroz šalu". Kad vas riječi prijatelja povrijede, potpuno je u redu da im to i kažete.
- *Širenje glasina ili laži o nekoj osobi ili grupi na internetu.* Kao što nećete povjerovati u sve što pročitate o životu poznatih glumaca i pjevača, tako nemojte misliti ni da je sve što na internetu vidite o drugima iz vašeg okruženja tačno.
- *Objavljivanje ili slanje slika ili video-snimaka sa ciljem da se neko ponizi ili osramoti.* Nekad se može dogoditi da iz nepažnje objavite sadržaj koji može povrijediti drugu osobu.
- Upućivanje prijetnji.
- *Korišćenje lažnih profila kako bi se širile uvredljive, ponižavajuće, zastrašujuće i povređujuće poruke.* Važno je da budemo odgovorni i u virtuelnom svijetu. Većina platformi pruža mogućnost prijave lažnih profila i savjetujemo vam da tu mogućnost koristite — na taj način stvaramo uređenije i zdravije onlajn okruženje.

Koje su posljedice sajberbulinga?

Onlajn zlostavljanje se na više načina može odraziti na mentalno zdravlje i život tinejdžera. Neke od posljedica su:

- slabiji uspjeh u školi i izostajanje s nastave - problemi u koncentraciji;
- povećanje stresa i anksioznosti;
- javljanje osjećaja usamljenosti i straha;
- pojava depresije ili depresivnih osjećanja;
- nisko samopouzdanje;
- u ekstremnim slučajevima sajberbuling može dovesti i do samoubistva.

Šta da uradite ako je neko od vaših prijatelja žrtva sajberbulinga?

Ne postoji savršena strategija za prevazilaženje ove vrste zlostavljanja. Ipak, ukoliko neko vama drag pati zbog zlostavljanja na internetu, najvažnije je da pokažete podršku i empatiju. Važno je da toj osobi pomognete da razumije da ona nije kriva. **Imajte na umu da je sajberbuling ozbiljan problem, zato nikada ne savjetujte prijatelju/prijateljici da „iskulira".** Takođe, ne govorite mu/joj da nije ništa strašno i da se uznemirava bez veze — jer jeste strašno!

Umjesto toga:

- Saslušajte šta ima da kaže.
- Ne krivite i ne osuđujte tu osobu zbog situacije u kojoj se našla.
- Stavite joj do znanja da znate kako se osjeća, čak i kad mislite da preuveličava. Ovdje mogu biti korisne rečenice tipa: „Vidim kako te to rastužuje/ljuti/frustrira/nervira...".
- Uputite je na druge ljude koji joj mogu pomoći, kao što su nastavnici, psiholozi, psihoterapeuti ili drugi profesionalci.

I na kraju, trudite se da prepoznate kako se vi osjećate, odnosno da li i vama treba podrška kako vas patnja prijatelja ne bi preko mjere uznemiravala.

Kako spriječiti da sami postanemo zlostavljači u sajber svijetu?

Svi ponekad volimo da „bacimo hejt" kad ne podržavamo ili ne volimo neki sadržaj na internetu. No u virtuelnom svijetu, baš kao i van njega, bilo bi sjajno poslušati savjet mudrog Sokrata i svoje riječi prosijati kroz tri sita. Naime, Sokrat savjetuje da se zapitamo: da li je to što želimo reći istinito, da li ćemo time učiniti nešto dobro i da li će to koristiti drugim ljudima. Ukoliko odgovor nije potvrdan u sva tri slučaja, vjerovatno će neko biti povrijeđen i bolje je odustati od namjere da se podijeli taj sadržaj.

V. Ketfišing – sajberbuling ili naivno trolovanje?

Da li se možete sjetiti koliko je najviše vremena prošlo a da ni s kim niste razmijenili par rečenica, bilo u onlajn, bilo u oflajn svijetu? Dvadeset četiri časa, jedna sedmica, mjesec dana? Sve su prilike da ta brojka ne prelazi više od par sati. Nije nam potreban nikakav glamurozan uvod niti naučni rad da bismo shvatili da je komunikacija prije svega naša neophodnost, pa tek onda rezultat konkretne potrebe za informacijom. Sposobnost međusobnog sporazumijevanja ljudi radi zadovoljavanja interpersonalnih, socijalnih, egzistencijalnih i drugih potreba stara je koliko i čovjek.

Već smo naučili sve o značaju komunikacije i činjenici da je ona, posebno u vrijeme pandemije koronavirusa, prenijeta u onlajn svijet. Sad vas pitamo: **da li ste, za sve vrijeme boravka u raznolikim internetskim nišama, imali makar jedno negativno iskustvo kad je riječ o onlajn komunikaciji?** Ako je odgovor potvrdan, znajte da niste jedini. S razvitkom interneta, procvatom društvenih mreža, dejting sajtova i raznoraznih oblika digitalne razonode, porastao je i broj onlajn prevara. U nastavku ćemo pokušati da vam približimo neke od rastućih problema kada je u pitanju komunikacije u digitalnom svijetu, ali i načine na koje se možete zaštiti.

Onlajn prevarant vs. ja – gdje je granica?

Da li ste ikada dobili zahtjev za prijateljstvo od profila za koji ste gotovo sigurni da je lažni? Ili, da odemo korak dalje: da li ste bili u prilici da razvijete komunikaciju s nekim koga uživo ne poznajete, a ispostavilo se da se ta osoba lažno predstavljala?

Da se razumijemo, u onlajn okruženju svi pomalo varamo. Provlačimo fotografije kroz filtere, brišemo tagove s fotografija/video-zapisa koji nam se iz nekog razloga ne dopadaju, tagujemo se na lokacijama na kojima možda nikada nismo bili. Koristimo nadimke ili alijase, kreiramo dodatne profile u cilju dobijanja tokena za igranje „Slagalice" ili neke druge igre kojom smo opsjednuti u datom trenutku. Po čemu se mi, onda, razlikujemo od ostalih internet prevaranata? Odgovor je jasan: za sve gorenavedene radnje postoje mnogi legitimni i opravdani razlozi. Dok god time što radimo ne ugrožavamo drugog i nikom ne nanosimo štetu, to je skroz OK. Dok god druge ljude ne zavaravamo fotografijama provučenim kroz filtere toliko da se naš lik zagubio, dok god ne uhodimo nekog s profila koji nam služi isključivo za dobijanje tokena, i dalje je OK. Dok god nam nadimak služi da zaštiti naš identitet i podatke, a nikako da ugrožava nekog, to je još uvijek OK. No, ako iskoračimo van ovih granica i kročimo na teritoriju na kojoj jasno nanosimo štetu nekim drugim licima, prešli smo na tamnnu stranu. A to skroz, sasvim, potpuno sasvim, nije OK. Zbog toga je jako bitno da upalite lampice i uvijek iznova sebi postavljate vrlo bitno pitanje: da li će moj postupak na neki način povrijediti, ponizitii ili omalovažiti drugu osobu? Ako je odgovor potvrdan, dalje djelovanje je jasno – obustavite misiju!

Ketfišing – naivno pecanje ili opasan ribolov?

Ljudi već eonima falsifikuju lična dokumenta, podatke, pa čak i novac (sjetite se samo legendarnog filma s Leonardom di Kaprijem iz 2002. godine – *Uhvati me ako možeš* (Catch me if you can)). No s nastankom i masovnom upotrebom interneta, ovaj trend bilježi značajan progres.

Jedan od sve rasprostranjenijih oblika internet prevara, a može se reći i jedan vid sajberbulinga, jeste ketfišing (*catfishing*). **Ketfišing predstavlja kreiranje lažnog identiteta na osnovu kog osoba koja ga je stvorila želi nešto od osobe (ili više njih) s kojom je u kontaktu.**

Sada ono pitanje o komunikaciji s nekim koga ne znate lično, već samo preko društvenih mreža, dobija potpuni smisao. Nažalost, ovaj oblik nasilja sve je više zastupljen, a ako ste imali slično iskustvo, imajte na umu da niste jedini. Među poznatim ličnostima je veliki broj onih koji su na ovaj ili onaj način bili žrtve ketfišinga, o ćemu možete pronaći mnoštvo materijala onlajn, i vjerujte na riječ — nema svaka priča potpuno srećan kraj.

Postavlja se pitanje šta je cilj osobe koja se lažno predstavlja, zbližavajući se sa osobom s kojom je u svakodnevnoj komunikaciji, pretvarajući se da dijeli ista interesovanja, probleme, svakodnevicu... **U velikom broju slučajeva ultimativni cilj zlostavljača jeste finansijski dobitak, ali nekada se sve svodi na kompromitovanje žrtve (na bilo koji način), ili čak na formu trolovanja.** MTV je 2002. godine lansirao rijaliti šou *Catfishing*, kako radi monetizacije rastućeg interesovanja o ovom vidu virtuelnog zlostavljanja, tako i u cilju podizanja svijesti o njegovom postojanju.

Najveći problem kod ketfišinga jeste činjenica da se žrtva ovakve prevare zaista veže za prevaranta. Prevarant prethodno odradi „domaći zadatak", tj. dobro istraži interesovanja osobe koju je odabrao za komunikaciju. Kada se upoznate s nekim preko društvenih mreža i razvijete pozitivnu komunikaciju, to nije nužno loša stvar. Naprotiv. **Ali ukoliko vam osoba prečesto govori ono što želite da čujete, saglasna je sa svim što napišete, priča vam o potresnom životnom iskustvu udarajući na empatiju, ili čak zatraži manju ili veću novčanu pomoć, to je već razlog za opravdanu sumnju.** Problem je u tome što je svako od nas sklon tome da bude zaslijepljen osjećanjima, posebno kad nam neko pruža mnogo više pažnje nego što smo navikli. U tim trenucima, bitno je zaustaviti se i razmisliti da li nas neko iskorišćava za sopstvene, više ciljeve, ili smo zaista razvili prijateljsku komunikaciju i obostrani osjećaj prisnosti. Čak i ako zaključite da je u pitanju ovo drugo, **nikada ne dijelite lične informacije, kao što su broj telefona, adresa stanovanja, podaci o bankovnom računu.** Vodite računa o sadržaju koji dijelite sa osobama iz virtuelnog svijeta (bilo u pisanoj, audio, foto ili video formi). Pričali smo već o tome da dugme „delete" na internetu baš i ne radi posao.

Opasnosti koje ketfišing nosi prevazilaze finansijske. Ovaj oblik prevare se može iskoristiti i da se osoba navede na upoznavanje uživo, nesvjesna da ima posla s prevarantom. **Potencijalna kidnapovanja ili nanošenje štete na bilo koji način najozbiljnija su posljedica ketfišinga.** Zbog toga, čak i ako se odlučite na upoznavanje s nekim koga poznajete samo preko društvenih mreža / sajtova za komunikaciju (što se, svakako, ne preporučuje), obavezno povedite još nekog s vama. Izbor javnog mjesta koje uvijek vrvi od ljudi se podrazumijeva, kako biste sve potencijalne opasnosti sveli na minimum.

Hvatanje hvatača – kako namirisati udicu?

Iako je nesporno da nas društvene mreže spajaju, moramo imati na umu da one istovremeno i destabilizuju sve ono što mislimo da znamo o osobi s kojom komuniciramo. **U najvećem broju slučajeva, osoba koja se bavi ketfišingom koristi ime ili identitetsku „podlogu" osobe koju poznaje ili ju je poznavala u stvarnosti.** Činjenica je da se na ketfišing lako upecati, ali to ne znači da se ova prevara ne može pravovremeno uočiti.

Prevarant uvijek koristi lažne podatke, kako informacije tako i fotografije. Ako sumnjate u namjere i iskrenost osobe s kojom ste u stalnoj onlajn komunikaciji, a koju nikada niste vidjeli uživo, Gugl pretraga fotografija (*Google Image Search*) je vaše prvo oružje. Provucite fotografiju te osobe kroz ovaj alat i dobro analizirajte rezultate pretrage. Ne zaboravite – žrtva ketfišinga nije samo osoba s kojom prevarant komunicira, već i osoba čiju fotografiju i podatke koristi. Jedan od načina borbe protiv ketfišinga jeste i odbijanje zahtjeva za prijateljstvo (na svim društvenim mrežama) od osoba koje ne poznajete, lično ili makar preko prijatelja ili rodbine. Ukoliko vam, iz nekog razloga, to ne odgovara, obavezno podesite opciju 'privatnost' na način da zaštitite sopstveni sadržaj. Možete odabrati da ono što objavljujete vide samo vaši prijatelji, ili, u slučaju da komunicirate s velikim brojem ljudi u onlajn svijetu, posebna grupa prijatelja koju sami odaberete. Na taj način filtrirate informacije koje dijelite sa svima od onih koje, ipak, ne treba da dopru do velikog broja ljudi.

Dobra taktika jeste i brisanje svih korisničkih naloga koje više ne koristite. Ukoliko vi sami ne koristite podatke i informacije sa nekog naloga, zašto biste to omogućavali drugima? Na koncu, opet ćemo ponoviti — nikada, nikada, nikada ne dijelite bilo kakve lične informacije sa osobama koje ne poznajete.

Ketfišing prevaranta nerijetko možete prepoznati i po lošoj gramatici, činjenici da vam je u nekom trenutku zatražio novac, priči o navodno lošem zdravstvenom stanju ili nekoj drugoj neprilici u kojoj se nalazi. Takođe, ukoliko odbija video-poziv ili je konekcija prividno jako loša (toliko da je lik osobe zatamnjen do neprepoznatljivosti), ima jako mali broj prijatelja i interakcija na društvenoj mreži preko koje komunicirate, tvrdi da nema stalnu adresu ili da je u inostranstvu – sve su to znaci da nešto nije kako treba i da je vrijeme za prekid komunikacije, makar dok ne dođete do preciznih podataka o osobi „s druge strane ekrana".

Naš cilj, kao savjesnih korisnika interneta, jeste da preduzmemo sve da ovakve vrste prevara svedemo na minimum. To, nažalost, nije uvijek moguće, ali je bitno poznavati alate i načine na koje se možemo odbraniti. Ukoliko shvatite da ste potencijalna žrtva ketfišinga – ne paničite. Odmah obustavite komunikaciju i sačuvajte sve prepiske (skrinšot) kako bi se prevarant što brže i preciznije identifikovao. Svakako uputite žalbu policiji, CIRT-u (*Computer Incident Response Team*) i korisničkoj podršci sajta/društvene mreže. Obavezno prijavite profil. Takođe, ne zaboravite da prijavite ukoliko ste podijelili bilo kakve lične podatke, kako bi se pravovremeno reagovalo na sve moguće zloupotrebe.

Granice onlajn komunikacije – da li ih ima i kako ih prepoznati?

Ketfišing je samo jedan od različitih oblika prevara na internetu. Od fišinga, preko „ko vam je gledao profil" linkova, poklon-kartica, vaučera, poklanjanja skupih brendova, do oglasa koji nude puno novca za rad od kuće ili poruke od daljih rođaka koji su se sjetili da su vam ostavili ogromno bogatstvo, sve do lažnih profila na društvenim mrežama, lažnih veb-sajtova koji vam reklamiraju proizvode po smiješno niskim cijenama....

Ne možemo dovoljno naglasiti koliko je bitno **da sve što vam se čini previše dobrim da bi bilo istinito (a obično se ispostavi da je baš tako), temeljno provjerite.** Kad je komunikacija u pitanju, to može biti malo teži zadatak, budući da je komunikacija, čak i u realnom svijetu, jako specifična. Zbog toga je izuzetno važno postavljanje granica. Na šta se tačno misli?

Kao što se u realnom svijetu nećete uključiti u razgovore koji vas ne interesuju, nećete ispratiti baš svaku prepirku, ili ćete se pak svjesno isključiti iz komunikacije koja je očigledno kontraproduktivna, tako treba znati kad je vrijeme da se nešto prećuti i onlajn. **Svaki oblik komunikacije koji, na bilo koji način i iz bilo kog razloga, čini da se osjećate neprijatno, potrebno je u startu prekinuti.** Jedna od nuspojava komunikacije koja se odvija tipkanjem po tastaturi, skrivanjem iza računara i u potpunom odsustvu fizičke note (koja i te kako stvara razliku), jeste novoformirana hrabrost koja proizilazi iz prividne anonimnosti. Ljudi znaju biti mnogo oštriji, zlobniji i više osuđivački nastrojeni iz udobnosti svojih fotelja nego prilikom komunikacije oči u oči. No, to nikako ne znači da vi treba da postanete, na bilo koji način, žrtva nečije prividne hrabrosti na internetu. Kako onlajn, tako i oflajn – sve što vam ne prija, jedan klik na „x" u gornjem desnom uglu (u oflajn svijetu ne baš tako, ali poenta ostaje) i spremni ste za povratak na sadržaje i/ili u komunikacije koje vam ne stvaraju nikakve neprijatnosti.

Granice su bitne zbog osjećaja sigurnosti, ali i slobode. **Empatija je srž komunikacije, a empatiju je u onlajn svijetu mnogo teže iskazati, a još teže iskreno osjetiti.** Bitno je da se u svakom trenutku ponašate savjesno i da ste svjesni da vaše ponašanje u virtuelnom svijetu nikome ne nanosi štetu. Ako se nađete s druge strane medalje i osjetite bilo kakvu nelagodnost, ne plašite se da se vratite unutar granica koje ste sami kreirali. Znate, ne zaslužuje svaka poruka da bude pročitana, a kamoli da se na nju odgovori. Neke granice su tu da bi se prelazile, a neke, poput ove, služe da nas zaštite i omoguće nam da uživamo u svom ružičastom parčetu interneta. I to je sasvim OK.

1. Lažne nagradne igre

Riječ je o prevarantima koji se lažno predstavljaju kao institucije (najčešće tako što prave lažne stranice banaka i trgovinskih lanaca na društvenim mrežama, ili tako što šalju cirkularne imejlove ili SMS poruke) i raspisuju nagradnu igru u kojoj je lako učestvovati (recimo „unesite broj 76 u komentaru"). Nakon što ispunite „kriterijum za učestvovanje", privatnom porukom vas obavještavaju da ste dobili nagradu i da im od vas treba „samo još nekoliko podataka". Ti podaci su najčešće: broj bankovne kartice, datum isteka kartice, CVC broj, vaše ime i prezime, matični broj, slika vaše lične karte ili računa za komunalije i slično. Ovi podaci su dovoljni da prevarant, uz manje ili više dodatnog truda, može da transferuje novac sa vašeg računa, ili pak da kupuje za sebe usluge plaćajući ih vašom karticom.

Razlog uvriježenosti ove vrste prevare velikim dijelom leži u odnosu društvenih mreža - službene naloge je gotovo nemoguće verifikovati, pa je korisnicima otežano razaznavanje pravih od lažnih naloga. Zato vam savjetujemo, savjetujemo da uvijek **provjerite postojanje neke nagradne igre na zvaničnom sajtu institucije koju osoba tvrdi da predstavlja, i da nigdje, nikad i ni s kim ne dijelite lične podatke na internetu. To se posebno odnosi na podatke poput matičnog broja, broja kartice ili korisničkog imena ili šifre za bilo koji nalog, jer legitimna institucija putem imejla, telefona ili društvenih mreža to nikada neće tražiti od vas.**

2. Fišing

Kako je svijest ljudi o tome da se povjerljivi podaci ne smiju dijeliti rasla, **prevaranti su došli na ideju da naprave sajtove koji izgledaju identično onima na kojima korisnici uobičajeno unose takve podatke, te da sakupljaju sve što oni unesu u odgovarajuće obrasce.** Ako žrtva vidi sajt koji izgleda identično kao Fejsbuk ili sajt njihove banke i ne posumnja da se radi o lažnom sajtu, refleksno će unijeti svoje podatke.

Ova metoda se u internet žargonu zove *fišing*. Gugl hrom i ostali moderni pretraživači imaju relativno pouzdanu, ali ne stoprocentnu zaštitu od fišinga, i preporučljivo je da redovno ažurirate svoj pretraživač. Dobar savjet je da *nikada ne unosite svoje pristupne podatke na link koji vam je neko poslao, već da u polje za pretragu ukucate adresu sajta na koji želite da se logujete.* Za sve naloge koji to podržavaju, uključite dvofaktorsku autentifikaciju, koja najčešće funkcioniše tako što osim korisničkog imena i šifre, treba unijeti i broj koji vam je prije prijavljivanja servis poslao SMS porukom (na taj način prevarant, osim vaših pristupnih podataka, mora imati i pristup vašem telefonu da bi pristupio vašem nalogu).

Menadžeri lozinki (*password managers*) poput LastPass-a (ili onoga koji je ugrađen u Gugl hrom ili Android)

mogu popuniti vaše korisničko ime i šifru za vas na sajtovima gdje ste već bili ulogovani. Ako u nekom trenutku nemaju podatak o tome da ste na nekom sajtu bili logovani, a inače te podatke pamte za taj sajt, to je znak da dvostruko provjerite vjerodostojnost sajta.

3. Prevara „ Učešće" (nigerijski princ, španski zatvorenik...)

Bilo da se radi o prijatelju koji je ostao zarobljen na aerodromu u Španiji, rođaku iz inostranstva koji vam je nenadano testamentom ostavio imovinu ili nigerijskom princu koji s ogromnim novcem bježi iz domovine, ova prevara uvijek ima isti cilj: da pred vas stavi izuzetno primamljivu stvar (uglavnom ogromnu svotu novca) koju ćete dobiti nakon što se premoste prve prepreke, za što je neophodno da vi onome ko će vam na kraju dati novac pošaljete neku svotu novca (nezanemarljivu, ali značajno manju od one koju ćete na kraju „dobiti") svotu novca.

Nakon što primi novac, prevarant se izgubi, ili pokuša da od vas izmami još novca. Jedno je sigurno: ni veliku nagradu, a ni svoj novac nikad više nećete vidjeti. Ova vrsta prevare nije nova, već se radi o modernoj verziji radnji koje su dokumentovane još u ranom devetnaestom vijeku.

Da biste izbjegli da postanete žrtva ove prevare, važno da imate na umu: koliko god ponuda bila primamljiva, **nikada ne šaljete novac nepoznatim ljudima.** Čak i ako poznajete osobu koja vam se javlja, provjerite njen identitet drugim putem (pozovite je telefonom, nađite se s njom...). Nije isključeno da je ta osoba žrtva krađe identiteta i da prevarant koristi njen identitet kako bi izmamio novac od vas.

4. „Dojave" i laka zarada

Prevarant se predstavlja kao neko ko ima „dojave" za sportske događaje koje će vam omogućiti da se obogatite u kladionici. Od vas se samo traži da - pogađate, platite neki mali iznos za te informacije. **Ova vrsta prevara posebno je sofisticirana, jer prevaranti koriste lažne profile na društvenim mrežama kako bi „dokazali" da su slične dojave imali u prošlosti, a pribjegavaju i statističkim proračunima kako bi došli do povjerenja optimalnog broja ljudi.** Fabrikovani profili, najčešće Tviter nalozi, u stvari su nalozi koji su bili ispunjeni stotinama predviđanja i iz kojih su izbrisana ona koja su bila pogrešna.

Da sve bude uvjerljivije, prvih nekoliko „dojava" dobijate besplatno. **„Besplatne dojave" su taktika segmentacije: prevarant šalje nasumična predviđanja raznim ljudima, gubi povjerenje većine za koju se ispostavi da su predviđanja pogrešna, ali dobija snažno povjerenje manjine kojoj je, pukom srećom, poslao ispravna predviđanja i kojoj će, na osnovu toga, papreno naplatiti dalja „predviđanja".**

Srećom, sama svijest o tome da ova vrsta prevare postoji, dovoljno je da se borite s njom. Prilika za laku zaradu na internetu ima gotovo uvijek, a kladioničarske dojave su apsolutno uvijek prevara.

5. „Cimanje"

Vidite propušten poziv s nekog čudnog broja telefona, uglavnom iz inostranstva. Kad pozovete da provjerite ko je i zašto zove, shvatate da ste dobili hotlajn broj s kojim svaki sekund razgovora papreno košta. Da stvar bude gora, puko nejavljanje na takav poziv nije potpuno siguran način da se odbranite. Hakeri su u stanju da naprednim metodama naplate takve pozive, čak i ako ih niste imali (dugi razgovori s takvim brojevima jednostavno se pojave na vašem računu).

Dobra vijest je da su naši telekomunikacioni operateri danas dobro upoznati s ovim prevarama, pa dug nastao pozivom koji niste napravili otpisuju uz žalbu i vrlo efikasno blokiraju pozive od prevarantskih brojeva i ka njima. Ipak, nije nemoguće da se neki zalutali poziv provuče i kroz njihove sigurnosne mjere (desilo se ove godine). **Ne uzvraćajte propušteni poziv ako vidite da je poslat sa čudnog broja ili broja iz inostranstva i žalite se ako je vaš račun veći od onoga što ste potrošili.**

6. „Imaš virus"

Porukom na društvenim mrežama, ili putem zastrašujućeg banera dobijate poruku da vaš računar ima virus ili sigurnosni propust. Srećom, firma koja je napravila propust ili zbog koje je virus instaliran na vaš računar ispraviće vaš problem besplatno.

Kad se javite (imejlom ili ostavljajući broj telefona na koji vas operater može zvati), dobijate instrukcije da instalirate određeni softver, ili da putem neke aplikacije za daljinsku kontrolu računara (*TeamViewer*, *Join.me* i sl.) date pristup njihovom operateru, koji će ispraviti grešku na vašem računaru. Iskustvo govori da je s vašim računarom najvjerovatnije bilo sve u redu - sve do jednog ovakvog trenutka, kad vi ili operater instalirate štetni softver. Od tog trenutka prevarant dobija pristup svemu onome čemu i vi pristupate sa svog računara i koristiće svaku priliku da iz toga izvuče što je moguće veću finansijsku korist.

Da biste se efikasno branili od ove vrste prevare, važno je poštovati dva pravila. **Prvo, ne instalirajte na svoj računar ništa u čiju namjenu i bezbjednost niste potpuno sigurni. I drugo, nikada ne dajte udaljeni pristup računaru nepoznatoj osobi, pa makar se ona predstavljala kao ekspert za bezbjednost u ogromnoj softverskoj kompaniji.**

Osim navedenih, na internetu prijete i stotine drugih prevara, a turbulentni ekonomski period pred nama vjerovatno će biti praćen i porastom pokušaja prevara. Za slučaj da ste postali žrtva prevare, ne krijte to nadajući se da će proći, već reagujte što brže, blokirajte bankovne kartice i prijavite prevaru nadležnim institucijama (policiji i CIRT-u).

Najbolji način da ostanete bezbjedni jeste da razmišljate svojom glavom. Nikad ne dijelite lične i pristupne podatke putem interneta — ni sa kim, makar bili potpuno sigurni da je taj neko vaš najbolji prijatelj. Koristite bezbjedan softver, uvijek imajte na umu da onaj s kim razgovarate možda nije ono što se predstavlja da jeste i znajte, da ako nešto izgleda suviše dobro da bi bilo istinito, vjerovatno nije istinito.

Hajde da sada ovaj primjer „prenesemo" na društvene mreže. Ukoliko vaš profil (na bilo kojoj mreži) nije zaključan, ili podešavanja privatnosti nisu na visokom nivou, bilo ko (ko vam nije prijatelj) može doći do većine potrebnih informacija prostom provjerom vašeg naloga. Objavljivanje informacija i događaja iz ličnog života, koje bi u realnosti većina ljudi zadržala za sebe ili podijelila samo s najbližima, u virtuelnom svijetu postalo je trend. Ova pojava nije nužno loša, no granica se mora postaviti. Da bi se to uradilo, **potrebno je da postanemo svjesni zbog čega je važna privatnost na internetu, ko nam je sve ugrožava i na koje načine.**

Kome su potrebni naši podaci?

Svaka aktivnost na internetu ostavlja digitalni trag — bilo da kreiramo sadržaj na društvenim mrežama, instaliramo aplikaciju, posjećujemo neki veb-sjat, igramo onlajn igru, ili koristimo internet pretraživač kao što je Gugl. Ono što za nama ostaje jesu informacije, lične, one koje sami podijelimo, ali i one koje nesvjesno ostavimo, poput naše aktivnosti na nekom vebsajtu (koje tekstove čitamo, na koji način obavljamo onlajn kupovinu, na koje oglase kliknemo i slično).

Ništa što podijelite na internetu nikada nije u potpunosti privatno. Čak ni aplikacije za razmjenu poruka, kao što su Vajber ili Fejsbuk mesindžer, nisu do kraja pouzdane. Komunikacija može biti presretnuta, poruke skrinšotovane. Zapitajte se koliko ste puta i sami iskoristili opciju 'skrinšot' kako biste neku prepisku podijelili s licima koja nisu u njoj učestvovala. Na taj način se kompromituje privatnost osobe čije se poruke trajno bilježe, dijele s drugima, a nerijetko i javno objavljuju. Zbog toga je jako bitno da poštujete dva glavna postulata. Prvi je da **nikada, nikada ne dijelite značajne lične informacije (u bilo kom formatu) putem društvenih mreža i drugih onlajn alata komunikacije.** Takođe, uvijek vodite računa o tome šta i kome šaljete, imajući na umu da je sve što ne biste voljeli da vidi iko drugi osim osobe kojoj pišete vjerovatno bolje ostaviti za konverzaciju uživo. Drugi postulat nalaže da nikada **ne ugrozite privatnost neke osobe skrinšotovanjem i dijeljenjem njenih privatnih poruka s drugima ako znate da ta osoba to ne bi željela.**

Nema besplatnog ručka. Kako smo već naveli, sve naizgled besplatne usluge kompanije naplaćuju prikupljanjem naših podataka. Sjetićete se da gotovo svaka internet stranica traži vašu saglasnost jer koristi kolačiće (*cookies*), datoteke koje sa veb-stranice prikupljaju podatke o vašem ponašanju na toj stranici – koje tekstove

čitate, kakav sadržaj vas interesuje, koliko dugo ste se zadržali na sajtu, da li ste kliknuli na neki od oglasa i slično. Kad ponovo posjetite isti veb-sajt, sadržaj na njemu biće prilagođen vašim interesovanjima (onome što su kolačići saznali o vama prilikom prve posjete). Ovo zapravo i ne zvuči loše. Umjesto da se zamarate pretragom predmeta vašeg interesovanja, sajt će sam to učiniti za vas. Pitanje je: na koji način i zbog čega? Prikupljeni podaci najčešće se koriste za analizu i kreiranje ličnih, socio-psihiloških profila korisnika, radi ciljanog plasiranja proizvoda ili usluga prilagođenog individualnim karakteristikama i potrebama korisnika, ali i radi prodaje drugim kompanijama ili trećim licima.

Lični podaci podrazumijevaju: ime i prezime, adresu stanovanja, fotografiju, imejl adresu, IP (Intenet Protocol) adresu, lokaciju, podatke koji služe za analizu profila korisnika, pol, godine, radnu sposobnost, finansijsko stanje, lična interesovanja, potrošačke navike itd. To je, dakle, ogromna količina podataka koju neko može imati o nama, i to samo zato što naša svijest o privatnosti na internetu još uvijek ne nadmašuje našu predstavu o brojnim prednostima koje su nam na raspolaganju dok olako klikamo „da" na sve što nas određeni veb-sajt/aplikacija pita.

Zloupotreba ličnih podataka, što u komercijalne što u institucionalne svrhe, nije novost. Na primjeru kompanije Fejsbuk možete shvatiti do kojih razmjera to ide, ali i koliko su podaci bitni za sve kompanije koje žive od interneta. Osim aktivnih (podaci koje sami korisnici ostavljaju) i pasivnih (podaci koje korisnici nesvjesno ostavljaju, npr. preko kolačića), kompanije se služe i trećom vrstom podataka, koja predstavlja kombinaciju prve dvije. Postoje algoritmi za analizu aktivnih i pasivnih podataka korisnika, a rezultati te analize svrstavaju se u novu, zasebnu grupu.

Glavni cilj prikupljanja ovolikog broja informacija o korisnicima jeste profit, odnosno prodaja proizvoda ili usluga. Fejsbuk jeste besplatna platforma, ali ona živi od prodaje oglasnog prostora kompanijama širom svijeta. Stoga podaci koje Fejsbuk posjeduje o svakom korisniku (u januaru 2020, Fejsbuk je imao 2,45 milijardi korisnika) mogu biti i te kako značajni u kreiranju oglasa koji će ciljati osobe za koje je najvjerovatnije da će kupiti određeni proizvod ili uslugu.

Osim targetiranja radi prodaje, naši podaci nerijetko služe u druge, manje lijepe svrhe. Sajberkriminalci će prevrnuti svaki kamičak interneta kako bi došli u posjed podataka koji im mogu poslužiti za različite malverzacije. Fišing napadi, imejlovi ili poruke sa sumnjivim fajlovima ili linkovima, samo su neki od načina koji mogu poslužiti trećim licima da dođu do podataka kao što su broj kreditne kartice, pasoša, adresa stanovanja i slično. Pomisao na to da neko koga ne poznajemo i ko može živjeti bilo gdje na zemljinoj kugli posjeduje naše lične podatke - više je nego jeziva.

Kako zaštititi privatnost na internetu?

Prvo i osnovno: to što se od vas traže određeni podaci ne znači da treba i da ih ustupite. Ako se, na primjer, pridružujete nekoj društvenoj mreži, vrlo jednostavno možete ograničiti kako količinu podataka koju dajete (od ličnog imena do lokacije, godišta, broja telefona i slično), tako i osobe kojima će ti podaci biti vidljivi. Pri kreiranju imejl naloga, nema potrebe da ispunjavate svako polje (informacije o polu, datumu rođenja itd.). **Ograničite se na pružanje informacija koje su zaista neophodne da biste koristili određenu virtuelnu uslugu.**

Prilikom posjete veb-sajtovima, vodite računa o tome da samo oni, a nikako treća lica, mogu prikupljati neophodne podatke preko kolačića. Ovo možete uraditi tako što ćete podesiti svoj internet pretaživač da automatski odbacuje kolačiće trećih strana. Tako se znatno smanjuje mogućnost krađe podataka i različitih malverzacija, koje se najčešće dese preko nekih lažnih oglasa prikazanih na internet stranici koju ste inicijalno posjetili.

Vodite računa o „jačini" lozinki koje koristite. Pobrinite se da one zaista štite vaše podatke i nikako ne koristite istu lozinku na više mjesta. Takođe, nikada ne koristite korisničko ime sa jednog naloga kao lozinku na drugom, jer povećavate šansu da neko preuzme vaše naloge. Kreirajte lozinke tako da se sastoje od kombinacije velikih i malih slova i brojeva, kako bi vaši nalozi bili što je moguće bolje zaštićeni.

Ukoliko se pitate da li je sadržaj koji dijelite na društvenim mrežama previše ličan, zastanite i pogledajte malo profile drugih ljudi, kako onih sa liste prijatelja, tako i onih koji nisu na njoj. Sve ono što vi možete pronaći o njima onlajn (datum rođenja, fotografije, lokacija) mogu i oni o vama. Imajte na umu da jednom kad vaše fotografije postanu dio virtuelnog svijeta, imate vrlo malo kontrole nad njihovom upotrebom. Podesite opciju 'privatnost' na društvenim mrežama tako da imate određenu kontrolu nad sadržajem koji plasirate. Ukoliko niste sigurni da je nešto vrijedno objave, naučite da se zaustavite. Dodatno, obavezno se odjavite sa svih naloga nakon što završite sesiju, bilo da se radi o društvenim mrežama ili raznim stranicama na kojima imate profil. Nikada naloge ne ostavljajte aktivne, jer tako predstavljaju još lakšu metu za različite napade.

Kad kliknete na link koji vas vodi ka nekoj internet stranici, provjerite da li počinje sa ***https*** ili sa ***http***. Dodatno „s" garantuje da je veb-stranica sigurna i kriptovana (vidjećete i zatvoreni katanac – nekad je pored, a nekad u donjem desnom uglu prozora). Obavezno redovno brišite kolačiće (ukoliko niste sigurni kako, Gugl će vam začas pokazati).

Pametno korišćenje interneta podrazumijeva sprovođenje svih dostupnih mjera zaštite. To se odnosi kako na server i provajdere internet usluga, tako i na nas korisnike, na ostavljanje povjerljivih informacija i ličnih podataka, pogotovo ako smo konektovani preko javne nezaštićene bežične mreže ili javnog računara.

Nemoguće je ostati neprimijećen na internetu (većina nas to i ne želi). To ujedno znači da je nemoguće u potpunosti zaštititi i kontrolisati našu privatnost. Ali, ne smijemo previdjeti značaj i ulogu privatnosti na internetu i moramo postati svjesni koliko je ona bitna. Zbog toga je potrebno usmjeriti **pažnju na pametno i oprezno ostavljanje podataka (ono što ne bismo rekli neznancu nema potrebe da dijelimo ni s nepoznatim ljudima u onlajn svijetu), na upravljanje aplikacijama (Uslovi korišćenja su detaljan i dosadan dokument, koga sitna slova čine još neprivlačnijim, no važno je da znate koje podatke dajete na uvid kompaniji koja je razvila aplikaciju), ali i ostalim uslugama.** Na taj način, količina i vrsta podataka koja ostaje za nama u virtuelnom svijetu i koja je dostupna svima, može se svesti na prihvatljivu i sasvim podnošljivu mjeru.

Navoručenije: Užvajte u blagodetima interneta, ali uvijek imajte na umu da vaša privatnost nema cijenu i da je niko neće štititi osim vas samih.

Sad kad smo se upoznali sa osnovama onlajn reputacije, verbalne i neverbalne komunikacije, te sajberbulingom, različitim vrstama internet prevara i značajem privatnosti, vrijeme je za mali predah. Skuvajte kafu, napravite zakusku i duboko udahnite. Sekunde nas dijele od toga da zaista shvatimo (i prihvatimo) kako sve što pročitamo na internetu NIJE nužno istina (FOTO VIDEO!).

VI. Posljedice lažnih vijesti – efikasno kreiranje panike i dipfejk sadržaj

Ako ste gledali seriju *Teorija Velikog praska* (The Big Bang Theory), sjetićete se epizode u kojoj je jedan od glavnih likova, nesuđeni MIT doktorand Hauard Volovic, u emotivnom rastrojstvu nakon raskida sa Lesli Vinkl. Dok manično prati njen Fejsbuk profil, nailazi na status u kom Lesli objavljuje kako ga je ostavila. Iznerviran, želi da pronađe način da kaže svima kako je on taj koji je ostavio nju, što zbunjuje njegovog druga i kolegu, Raža, jer je Lesli napisala istinu. Vidno revoltiran i uvrijeđen, Hauard izgovara: „Istini nije mjesto na internetu".

Danas, 2020. godine, potpuno smo svjesni da je Hauardova izjava bila sasvim na mjestu. U moru vijesti najrazličitijeg sadržaja, koje nam se plasiraju putem tradicionalnih onlajn medija, sve je više onih koje su lažne. Imali smo priliku da vidimo i/ili pročitamo na koji je način širenje lažnih vijesti u doba pandemije COVID-a-19 prijetilo da nanese više štete od samog virusa. Zbog toga je jako bitno da se upoznamo s konceptom lažnih vijesti (fake news), saznamo kako da utvrdimo istinitost sadržaja koji nam se plasira, ali i da se detaljno informišemo o posljedicama koje lažne vijesti nerijetko ostavljaju za sobom.

Lažne vijesti u vrijeme pandemije koronavirusa – efikasno kreiranje panike

Kad konzumiramo neki sadržaj, treba da budemo sigurni u njegovu istinitost, relevantnost i pouzdanost. U tome nas sve češće sprečavaju **lažne vijesti, tj. namjerno plasirane dezinformacije ili teorije zavjere koje se šire preko tradicionalnih i/ili onlajn medija.** Da se odmah poslužimo konkretnim i relativno svježim primjerom. Kad je koronavirus zvanično „ušetao" i na našu teritoriju, životi su nam se promijenili u par dana. Prinuđeni da veći dio vremena provodimo kod kuće, bili smo na meti raznoraznih vijesti, od kojih je ogromna većina bila lažna.

Mogli smo da čujemo i pročitamo apsolutno sve – od „pet sigurnih znakova da imate koronavirus", preko „tri sastojka koja ima svako domaćinstvo liječe koronu", do informacija o skrivanju broja oboljelih, preminulih i slično. Slična situacija je bila i u svijetu. Sjetimo se situacije u Iranu: prema izvještaju iranske Vlade, u toj zemlji je od 20. februara do 7. aprila ove godine od trovanja alkoholom preminulo više od 700 ljudi, jer su vjerovali da je „metanol" zapravo lijek za koronavirus. Prije nego što unaprijed osudimo ljude koji su povjerovali u ovakvu vijest, sjetimo se da je snaga lažnih vijesti mnogo veća nego što se isprva čini, a time i njihove posljedice.

Poruke tipa: „Drug mog kolege, čija žena radi u Kliničkom centru, kaže da i kod nas postoje pozitivni slučajevi, ali da će zvanično objaviti za tri dana", ili: „Nezvanična informacija, od mog rođaka koji radi u Upravi policije, jeste da će Podgoricu zatvoriti u petak, ali to će objaviti tek u četvrtak", našle su svoj put do maltene do svih građana Crne Gore — ne samo putem društvenih mreža, već i preko SMS poruka ili preko Vajber komunikacije. Činjenica da veliki broj nas nije detaljno upućen u koncept lažnih vijesti dovela je do njihovog procvata u eri pandemije virusa. Brzina prenošenja lažnih vijesti, pogotovo putem onlajn kanala i medija, ide na ruku lakom kreiranju panike. Panika sa sobom nosi niz poteškoća i pritisaka, koji, posebno u vrijeme pandemije, mogu da ostave ozbiljne posljedice. **U kriznim situacijama, lažne vijesti dovode do narušavanja povjerenja u zvanične institucije – državu, ljekare, farmaceute. Dodatno, one pogoduju izgradnji lažnog osjećaja sigurnosti** (vijesti o „učinkovitim, prirodnim" ljekovima), čime nas dovode u neposrednu opasnost.

Naravoučenije: **Informacije iz nepouzdanih izvora (bilo da je riječ o medijima ili o tekstualnim porukama) nikada ne treba uzimati zdravo za gotovo.** Konkretno, u slučaju pandemije koronavirusa, provjereni izvori s relevantnim i tačnim informacijama jesu zvanični nalozi i veb-sajt Svjetske zdravstvene organizacije, Instituta za javno zdravlje Crne Gore, Nacionalnog koordinacionog tijela za zarazne bolesti Crne Gore i Vlade Crne Gore. Sve vijesti o pandemiji koje dolaze iz nekih drugih izvora potrebno je preispitati i nikako ne širiti dalje ukoliko nismo u potpunosti sigurni da je informacija tačna i provjerena.

Šta je dipfejk sadržaj?

Postoji nekoliko osnovnih razloga zbog kojih lažne vijesti jako brzo dobijaju na popularnosti. Prva je, naravno, brzina prenošenja informacija preko onlajn medija. Zatim sljede karakter same vijesti, koja je nerijetko senzacionalistička i u skladu s gorućim temama, kao i nedovoljna upućenost ljudi u koncept lažnih vijesti (*fake news*).

Prema istraživanju UNICEF-a i AEM-a [2],51% roditelja i 62% djece nikada nisu čuli za termin fejk njuz, a još veći procenat njih na zna značenje tog termina. Upravo je zato posebno važno shvatiti značaj ovog fenomena. Postoji više kategorija lažnih vijesti, kao što su „klik-bejt" (*click-bait*), propaganda, satira, zavaravajući sadržaj, nemarno novinarstvo i pristrasne vijesti — više o tome možete pročitati u tekstu „Prepoznavanje lažnih vijesti...", dostupnom na sajtu Digitalizuj.Me.

Pošto smo se bolje upoznali s lažnim vijestima i posljedicama koje one nose, preći ćemo na njihov sve popularniji oblik, tzv. dipfejk (*deepfake*). **Pojam je nastao kombinacijom riječi „deep" (duboko) i „fake" (lažno), a označava naprednu tehnologiju, zasnovanu na vještačkoj inteligenciji pomoću koje se mijenja postojeći i stvara novi (najčešće video) sadržaj, s ciljem prikazivanja nečega što se nije zaista dogodilo.** No, da se ne bismo gubili među vrtoglavim definicijama, poslužićemo se Jutjub videom. Džim Meskimen, poznati holivudski imitator, napravio je koristeći aplikaciju DeepFaceLabs interesantan video, koji na Jutjubu možete naći pod naslovom: *Deep Fake VFX - Deeper metrics of Christmas by Jim Meskimen*.

Kao što možete vidjeti, video je zabavnog karaktera i njegov krajnji cilj je naša ocjena kvaliteta Meskimenove izvedbe, imitacije poznatih glumaca. Ipak, ne možemo a da ne primljetimo koliko je postalo lako kreirati dipfejk sadržaj, pa se nameće pitanje kako da znamo čemu uopšte više možemo vjerovati. Iako je koncept lažiranja fotografija odavno poznat i široko rasprostranjen (Fotošop, Fejstjun), sve do kraja 2017. godine video je bilo mnogo teže izmijeniti na način da uvjerljivo prikaže nešto što se nije dogodilo. **Pošto se dipfejk sadržaj kreira uz pomoć vještačke inteligencije, koja iz minuta u minut napreduje i postaje sve savršenija, a korisnička osnova sve jednostavnija, došli smo do toga da svako može izmijeniti lica aktera, tj. kreirati dipfejk sadržaj.** A to je, sve su prilike, alarm za uzbunu.

Popularizacija ove forme lažnih vijesti, od 2017. godine nadalje, dovela je do toga da je danas zaista teško prepoznati šta je stvarno, a šta nije. Nadmoć videa u odnosu na tekstualni sadržaj uveliko doprinosi ovom problemu. Samo razmislite – mnogo ćete teže povjerovati u nešto što je neka javna ličnost saopštila ukoliko to pročitate nego ako to i vidite. Dodatno, nekad je lažna vijest toliko šokantna ili upečatljiva (bilo u video, bilo u pisanoj formi) da, čak i ako znate ili saznate da vijest nije istinita, ostaće vam dugo u pamćenju, a nakon nekog vremena nećete moći ni da se sjetite da li je u pitanju dezinformacija ili najčistija istina. E, u tom grmu i leži opasnost! Uz sve to, kreiranje dipfejk sadržaja omogućeno je svakom, preko softvera koji se može besplatno preuzeti. Ako znamo da nemaju svi ljudi u onlajn svijetu dobre namjere, opasnosti ove vrste tehnologije postaju nam sve jasnije.

Krajem 2017. godine, korisnici aplikacije Redit, nazvani dipfejks, koristili su dipfejk tehnologiju kako bi u javnosti plasirali lažne pornografske snimke poznatih ličnosti. Pošto znamo koliko ovi lažni video-snimci mogu izgledati vjerodostojno, jasno je kakvu su pometnju dipfejks izazvali. Razlozi za plasiranje ovakvog su mnogobrojni - od namjere da se zaradi novac, slava, do korišćenja ovih falsifikata u političke svrhe. **Softver na kome počiva dipfejk tehnologija izučava govor tijela određene osobe, njenu facijalnu ekspresiju, pokrete i slično, što pomaže u kreiranju ove forme lažnih vijesti.** U istraživanju koje je objavio Samsungov AI centar iz Moskve, zajedno sa Institutom za nauku i tehnologiju Skolkovo, objašnjeno je da je dipfejk video moguće kreirati uz pomoć jedne statične fotografije. Ukoliko se ovakva vrsta sadržaja plasira u cilju zabave i ne prelazi određene granice, nema razloga za strah, no kad ona postane alat za laganje i narušavanje tuđe privatnosti, onda imamo ogroman problem.

Opasnosti dipfejk sadržaja

Osnovna opasnost dipfejk sadržaja jeste to što **ljudi bez razmišljanja prihvataju da su stvari prikazane video-sadržajem istinite.** Za razliku od teksta ili fotografije, čija se vjerodostojnost češće dovodi u pitanje, video-sadržaj uživa veće povjerenje, koje najvećim dijelom počiva na uvjerenju da je takav sadržaj teže izmijeniti.

Druga opasnost koju dipfejk donosi jeste opšte **narušavanje kredibilnosti video sadržaja** – ljudi neće vjerovati ničemu, jer ne uspijevaju da razlikuju lažnjak od originala. Ili, ukoliko gledaju nešto što je u skladu s njihovim stavovima i uvjerenjima, pogotovu ako je u pitanju govor osobe u koju imaju povjerenja, biće spremni da povjeruju u istinitost video-sadržaja iako postoji realna sumnja u njegovu vjerodostojnost. Sve to može imati ozbiljne posljedice, posebno ako se (lažni) govor sastoji iz segmenata netrpeljivosti, poziva na sukobe, širenja mržnje prema onima koji ne zastupaju iste stavove.

Treća (nažalost, ne i posljednja) opasnost jeste **narušavanje ljudskih prava i sloboda.** Zamislite da neko kreira dipfejk video s vašim likom (čak i da je zabavnog karaktera), koristeći vaše fotografije i ne tražeći vaš pristanak. Osim što su vam jasno narušena prava i slobode, prinuđeni ste da dokazujete vjerodostojnost (odnosno nedostatak vjerodostojnosti) sadržaja, objašnjavate porodici/prijateljima o čemu je riječ, suočavate se s osjećanjima neprijatnosti i poniženja koja ničim niste zaslužili.

Iako ćete, ploveći internetskim okeanom, pronaći veliku količinu zabavnih dipfejk sadržaja, bitno je da ne zaboravite na opasnosti koje oni nose. Suočeni sa stvarnošću koja je istkana od mnogobrojnih niti lažnih vijesti, važno je da konstantno preispitujemo sve što gledamo i slušamo. Zapitajte se da li poznajete osobu (ili medij) koja je kreirala sadržaj, možete li pronaći relevantne podatke o autoru, kakva je poruka sadržaja koji se plasira, da li se ista vijest može pronaći kod više različitih izvora i slično. Čak i bez dipfejk sadržaja, u vremenu kad svako može pisati na internetu šta god želi, **ne smijemo svaku informaciju koju pročitamo automatski smatrati činjenicom.** Zabavni sadržaj je jedna stvar, ali kad su u pitanju ozbiljne, a posebno zlonamjerne informacije, važno je pronaći kredibilne izvore i ne povjerovati u sve što vidimo ili pročitamo. Što bi Alastor Ćudljivko, profesor Odbrane od mračnih vještina (poterovci među vama će se odmah sjetiti) rekao, a što posebno važi za pristup lažnim vijestima i dipfejk sadržaju na internetu: „Stalan oprez!"

VII. Uravnotežena upotreba tehnologije

Konstantno provjeravamo telefone. Što ih više koristimo, kao da nas više „zovu". Slično se ponašaju i ljudi oko nas. Da li ste se ikada zapitali šta nas to tjera da opsesivno gledamo u ekrane, vješto izbjegavajući nedjeljne izvještaje o korišćenju telefona, do kojih vrlo lako možemo doći.

Sve je počelo od biznis-modela nekoliko najuticajnijih i najbogatijih kompanija na svijetu

Od čega žive Fejsbuk, Gugl, Jutjub, Epl, Fortnajt?

Kompanije kao što su Fejsbuk (uključujući i Instagram i Vocap), Epl, Gugl (uključujući i Jutjub), Snepčet, Rovio, ili Epik (Fortnajt) zarađuju od toga koliko ljudi koristi njihove proizvode. Kad kažemo „koliko", mislimo na broj ljudi, ali i količinu vremena koje ti ljudi izdvajaju. Ove kompanije žele naše oči (i ruke) na njihovim proizvodima. Često se u naučnoj javnosti nazivaju majstorima manipulacije, jer zbog velikog broja korisnika mogu da testiraju ponašanje korisnika i u prilici su da naprave svoje servise tako dobrim da ljudi ne mogu da prestanu da ih koriste.

Najveći dio prihoda Fejsbuka i Gugla potiče od reklamiranja. Reklama se naplaćuje po kliku ili po impresiji. Većina društvenih mreža su besplatne i zarađuju od reklamiranja.

Video-igra Fortnajt, u vlasništvu Epik gejmsa, besplatna je. Poput mnogih drugih, Fortnajt (Epik gejms) zarađuje tako što nudi svojim igračima opciju da plaćaju mjesečnu pretplatu, ili da kupe digitalnu valutu (*V-Bucks*) kojom plaćaju određene dodatke kroz igru i kroz niz mikrotransakcija.

Što više koristimo proizvode ovih kompanija, što više vremena provedemo skrolujući i klikćući i pregledajući, oni više zarađuju, bez obzira na to da li ih plaćamo ili ne. Zato se kaže da je na prodaju naša pažnja i svi ovi servisi bore se upravo za nju.

Pomenute kompanije zapošljavaju timove psihologa, neurologa, inženjera i bihejvioralnih eksperata, kojima je jedini posao da pronađu način da aplikacija koju nam nude bude što privlačnija i da korisnici provode što više vremena koristeći je. Oni mijenjaju naše navike i to ne rade slučajno, nego s namjerom, jer zarađuju na našoj potrebi i navici da koristimo njihove (besplatne) servise. Kao što duvanska industrija želi da što više ljudi puši, tako i tehnička industrija želi da mi što više koristimo njihove proizvode.

Zašto pametni telefoni i tehnologije uopšte imaju takav uticaj na nas?

Ponekad je naš odnos prema telefonu najsličniji onom što Golum iz Gospodara prstenova (italikom) osjeća prema svom prstenu. Psiholozi su ovu pojavu nazvali **nomofobija (no-mobile) — strah od gubitka telefona.**

U posljednje vrijeme, sve je veći broj psihologa koji kao pretjeranu upotrebu mobilnih telefona vide kao zavisnost sličnu kockanju. Oni ukazuju i na to da se prilikom korišćenja telefona, društvenih mreža, igranja onlajn igara, ili beskrajnog skrolovanja Instagramom i upadanja u tzv. crnu rupu Jutjuba, ljudi ponašaju slično kao korisnici droga. Teži slučajevi zavisnosti od telefona uključuju nesanicu, slabije fokusiranje i apatiju, a kad takve osobe nemaju pristup mobilnom telefonu, često reaguju bijesom ili depresijom, što su simptomi koji obično prate proces odvikavanja od droge.

Ako sve ovo znamo, kako to da se i dalje ne možemo odvojiti od telefona? Da li je u pitanju navika koju smo svjesno usvojili, ili pak nešto što nam se nameće i mimo naše volje?

Šta je navika, kako se stiče i od čega se sastoji?

Navika je ustaljeni način ili oblik ponašanja koji se ponavlja rutinski i obično nesvjesno. Sa stanovišta psihologije, **navika je manje-više tačno određeni način razmišljanja, ponašanja, potrebe ili osjećanja, koji se stiče prethodnim ponavljanjem ili ponovljenim mentalnim iskustvom.** Često nismo svjesni ponašanja koje spada u naviku jer obično ne razmišljamo o onome što rutinski radimo. Po nekim istraživanjima (*Wood, 2002*), 43% našeg ukupnog ponašanja u toku dana čine navike. Kao što znamo, stare navike se teško gube, a nove se jednako teško stiču. To je zato što se radnje koje ponavljamo urezuju u naš nervni sistem. Većina automatskih ponašanja imaju iste osobine: efikasnost, nesvjesnost, nedostatak kontrole, nenamjerne su.

Navika inicijalno može biti pokrenuta s ciljem, ali cilj vremenom gubi smisao. Povremene i nesigurne nagrade su posebno efektivne u podsticanju navika. **Formiranje navika se sastoji iz tri komponente: okidač, ponavljanje i nagrada.**

Kad želite da steknete novu naviku, nastojte da kreirate sebi okidač i nagradu. Na primjer, ako želite da počnete da trčite, planirajte da to radite uvijek u isto vrijeme u toku dana, da bi dnevna rutina bila okidač. Obucite se što prije da ne biste izgubili zalet, pođite na trčanje i odredite nešto čime ćete se nagraditi kad završite. Recimo, ukusnim čokoladnim kolačem. To određivanje nagrade je mnogo važnije nego sama nagrada, čokoladni kolač na kraju i nije toliko bitan. Jednom kad steknete naviku, cilj (nagrada) gubi smisao. Dovoljna nagrada postaje sama činjenica da tu naviku praktikujete.

Kako tehnologija utiče na naš mozak?

„Tehnologija nije droga. Ali svakako može tako da se posmatra, jer radi i utiče na nas na isti način i ima iste rezultate", rekao je Robert Lustig, pedijatar i profesor na Univerzitetu Kalifornija. U svom istraživanju, on se bavi reakcijama koje izazivaju zavisnost u mozgu (bila ta zavisnost od šećera, heroina ili tehnologija).

Neumjereno korišćenje tehnologije izaziva stres koji ima dvostruke negativne efekte na naš mozak. Prvo, povišeni nivo stresa izaziva višak kortizola, koji može da ošteti neurone u dijelu mozga je zadužen za sjećanja (hipokampus). Drugo, stres deaktivira prefrontalni korteks - izvršni dio mozga koji obično reguliše i ograničava lučenje dopamina i osjećaj zadovoljstva ili nagrade. Ukratko, kad se mozak navikne na veće doze dopamina, on zahtijeva veću dozu. Dr Lustig je primijetio da su adolescenti posebno osjetljivi jer je prefrontalni korteks dio mozga koji se najkasnije formira, odnosno kreira određenu zaštitu oko neurona. Zbog toga su tinejdžeri najskloniji rizičnom ponašanju.

Poznato je da hemijska zavisnost počiva na sposobnosti psihoaktivnih supstanci da povećaju nivo dopamina u mozgu. **No naučnici su otkrili da varijabilne nagrade koje postoje u kockanju i video igrama takođe izazivaju uvećanje dopamina.** Na primjer, narkotici će konzistentno izazivati osjećaj nagrađivanja u mozgu zavisnika. Sličan proces dešava se i u mozgu osobe koja ne zna da li će pobijediti u video-igri, u kockanju, ili čak da li će dobiti lajk – **ta nesigurnost povećava intenzitet fiziološkog odgovora na nagradu.**

Šta zapravo znači balansirana upotreba tehnologije?

Balansirana upotreba tehnologije predstavlja sposobnost da upravljamo svojim životom (i onlajn i oflajn) na uravnotežen način. To podrazumijeva samokontrolu u pogledu vremena provedenog pred ekranom, u multitaskingu i interakciji s digitalnim medijima i uređajima.

Potrebno je **da razumijemo prirodu i uticaj korišćenja tehnologije (pretjerano korišćenje telefona, multitasking) na naše zdravlje, produktivnost i stil života, kao i da steknemo znanje neophodno da bismo se uhvatili u koštac sa štetnim uticajima tehnologije.**

Potrebno je da imamo sposobnost da razvijemo vještine upravljanja vremenom i resursima da bismo izvršili zadatke.

Da li je tehnologija dobra ili loša za nas?

Gugl i Epl imaju aplikacije za praćenje vremena provedenog pred ekranom i postavljanje vremenskih ograničenja za određene aplikacije.

Potreba da stalno provjeravamo poruke, želja da budemo vrlo aktivni na društvenim mrežama, nemogućnost skretanja pogleda sa Jutjub sadržaja ili izlaska iz fantastičnog svijeta video-igara, nisu ništa drugo do manifestacije stanja koje upućuje na simptome psihijatrijskih poremećaja kao što su OKP, narcisizam, zavisnost i ADHD, koji se manifestuju kroz upotrebu tehnologije. To stanje se zove ***iDisorder***. Ipak, mnoga istraživanja ukazuju na to da je priča o depresiji, agresivnosti, usamljenosti, zavisnosti i narcisizmu kao posljedicama neumjerene upotrebe tehnologije —pretjerana.

Iako se određena ponašanja do kojih dolazi pod uticajem tehnologije mogu klasifikovati kao poremećaj, ne treba smetnuti s uma da taj uticaj, osim negativnih, ima i svoje pozitivne strane.

Negativne strane

1. Multitasking - Distrakcija

Oni koji *multitaskuju*, tj. istovremeno obavljaju više poslova/radnji, često preskaču sa zadatka na zadatak i samim tim lošije obavljaju te zadatke. Učenje je moguće jedino ako je telefon isključen ili je daleko, odnosno ako ne razmišljamo o tome je li neko nešto lajkovao ili poslao poruku.

2. Očekivanja ubrzanog zadovoljstva (instant gratification)

Na emotivnom nivou, postavljanje selfija na društvenim mrežama podstiče našu potrebu za pažnjom i očekujemo potvrdu. Navikli smo se na tu vrstu ubrzanog zadovoljstva, što dovodi do toga da i u životu počnemo da se ponašamo na isti način - ako ne možemo da postignemo da nas neko pohvali, osjećamo se loše. Ako ne pobijedimo u igri u oflajn svijetu, osjećamo se mnogo gore.

3. Nestrpljivost

Tehnologija je sve brža, a naša pažnja sve kraća. Koliko smo strpljivi da sačekamo da se video učita? Dvije sekunde. Koliko teksta imamo živaca da pročitamo? Dvadeset posto.

4. Narcisizam

Bez obzira na to što nam postavljanje fotografija pomaže u društvenom životu, ono podstiče tzv. me-centered mentalitet. Narcisizam je kombinacija egzibicionizma i osjećaja da nam pripada više nego što je to slučaj. Istraživanja jasno povezuju ova dva osjećaja s količinom postavljenih ličnih sadržaja na društvenim mrežama i *samopromocijom*, a onda i reakcijama.

5. Kognitivni gubici

Prema istraživanjima, osobe koje imaju *Internet Addiction Disorder* (IAD) imaju smanjen tzv. sivi dio mozga, ali i tzv. dio, koji je povezan *s kognitivnom kontrolom* i ponašanjem koje upravljanja ciljevima. Oštećenje se dovodi u jasnu vezu s količinom vremena provedenog na internetu.

6. Osjećaj izolacije

Puno se priča o negativnom uticaju tehnologije na naš osjećaj izolovanosti i usamljenosti. Ipak, jedno od najvećih istraživanja Pju centra ukazuje da internet i tehnologija, iako odvlače ljude od drugih ljudi u fizičkom smislu, ne čine ih usamljenima. Naprotiv, internet i tehnologija podstiču društvene interakcije.

Oni koji najbolje koriste tehnologiju:

- brzo pronađu informaciju o svemu što ih zanima;
- brzo uče;
- brzo razaznaju da li je nešto laž ili ne;
- mogu da kontrolišu svoje digitalno zdravlje;
- nisu nestrpljivi;
- ne gube koncentraciju lako;
- ne treba im telefon da ih konstantno zabavlja.

Pametno korišćenje pametnih telefona

Matematičar, fizičar i inžinjer Lord Kelvin jednom prilikom je rekao: „Ako nešto ne može da se izmjeri, ne može ni da se poboljša."

Primijenimo to i na korišćenje telefona:

- Ajfon — namjestimo skrin tajm (Screen time)
- Android — digitalna dobrobit (Digital wellbeing)

Zavisnost od različitih supstanci poznata je hiljadama godina, ali smo tek u posljednje dvije decenije postali zavisni od tehnologije. Od Instagrama, Fejsbuka, Netfliksa, imejla, društvenih mreža i platformi koje koristimo u cilju poboljšanja kvaliteta života... Ne mogu se poreći dobre strane tehnologije, ali treba biti svjestan da privlačnost raznovrsnih platformi i aplikacija nije slučajna. Iza svakog od pomenutih servisa stoje timovi stručnjaka koji su posvećeni tome da nas „natjeraju" da što više vremena provedemo koristeći njihove aplikacije. Na taj način nas upoznaju, te nije ni čudo što nas isti oglasi prate po internetu danima, što Instagram „zna" koju smo odjevnu kombinaciju mjerkali na Asosu, a par puta smo se mogli zakleti da nas sopstveni telefon prisluškuje. O čemu je tu riječ?

VIII. Industrija internet oglašavanja: kako to Instagram zna koje patike želiš za rođendan?

Koliko puta vam se desilo da posjetite neku veb-stranicu, a da vas nakon toga oglasi s te stranice danima prate, po svim postorima interneta koje obilazite?

Da li vam se ikada desilo da pomislite kako vas telefon sigurno prisluškuje — jer kako bi inače znao da baš sada razmišljate o kupovini najnovije Plejstejšn konzole?

Ukoliko bar jednu od navedenih situacija prepoznajete iz sopstvenog iskustva, nastavite sa čitanjem. U tekstu koji slijedi nastojaćemo da vam približimo industriju onlajn oglašavanja, kao jedan od glavnih faktora koji oblikuju internet čineći ga onakvim kakvog ga znamo.

Ako ne plaćaš proizvod, ti si proizvod

Društvene mreže nam pomažu da prevaziđemo geografske i prostorne barijere, da ostanemo u kontaktu s prijateljima i porodicom gdje god se nalazili, da budemo u toku sa dešavanjima širom svijeta, da malo lakše podnesemo ograničenja kretanja i neizvjesnost s kojom se danas suočavamo.

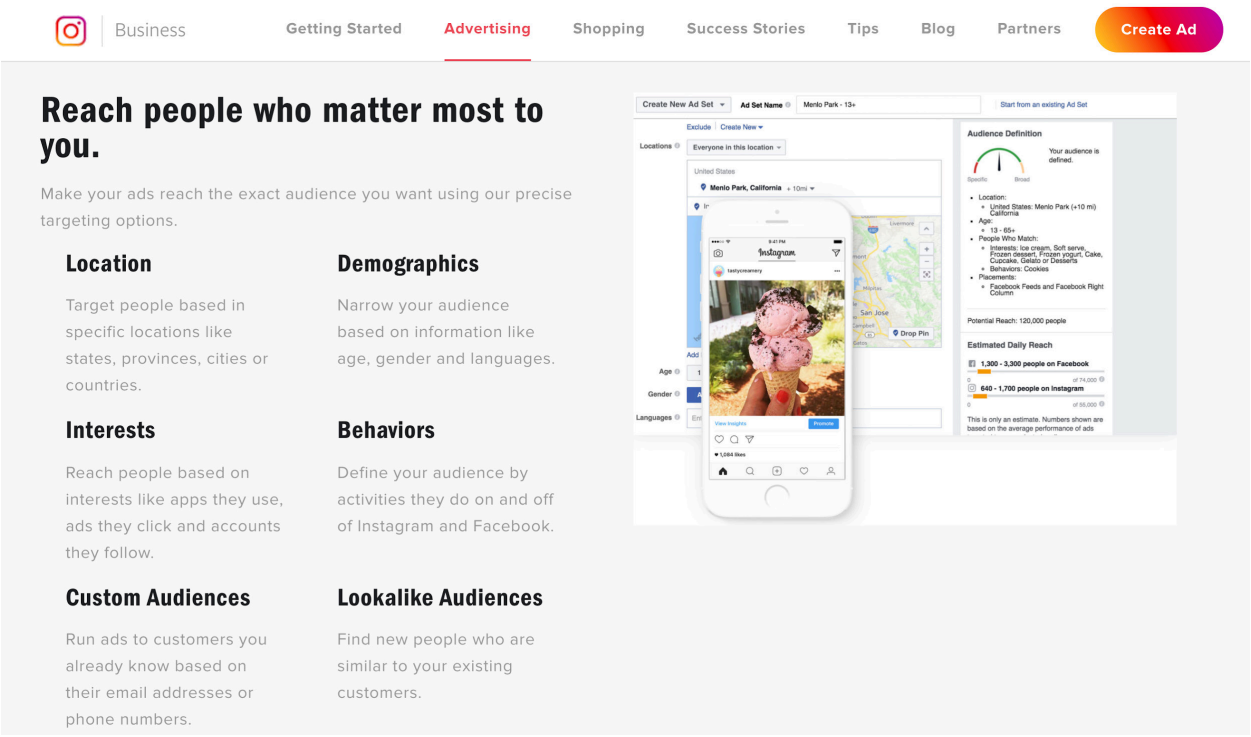
Iz dana u dan, preko 2,6 milijardi korisnika Fejsbuka, i dalje najpopularnije društvene mreže na svijetu, koristi ovu platformu da podijeli djelić svog svijeta s drugima i dođe do informacija koje su im potrebne. **Ukoliko uzmemo u ozbir da na svijetu ima 7,8 milijardi stanovnika, to znači da korisnici Fejsbuka čine 30% svjetske populacije.** Pri tome, u tu brojku nisu uključeni korisnici Instagrama i Vocapa - aplikacija koje sigurno koristite, a koje su u vlasništvu Fejsbuka.

Ovolikoj popularnosti društvenih mreža doprinio je veliki broj faktora, a jedan od možda najbitnijih jeste njihova „besplatnost" - svako ih može preuzeti i napraviti svoj profil. Međutim, moramo biti svjesni da **sistem koji opslužuje skoro tri milijarde korisnika ima velike troškove i zahtijeva velika ulaganja da bi nastavio da funkcioniše.** Fejsbuk, Instagram i ostale društvene mreže najvećim dijelom posluju na osnovu prihoda od kompanija koje se oglašavaju na tim onlajn platformama.

Drugim riječima, društvene mreže jesu besplatne u smislu da ne moramo novcem platiti njihovo korišćenje, ali samim posjedovanjem profila na Fejsbuku postajemo dio platforme koja kompanijama naplaćuje svoj prostor - ali i pristup nama. Na neki način, time proizvod postajemo upravo mi.

Svaka naša aktivnost na Instagramu, nalozi koje pratimo, video-snimci koje gledamo, pojmovi koje pretražujemo, baš svaki klik **pomaže sistemu da nas bolje upozna i da upotpuni naš „korisnički profil".** Kao rezultat toga, na svom Instagram fidu vidimo postove ljudi i kompanija koji nas zaista interesuju, sadržaj koji nam platforma plasira je personalizovan, prilagođen nama (meni, tebi) i navodi nas da pretražujemo još malo... i još samo malo. Isti podaci se koriste i za plasiranje oglasa. Naime, što Instagram bolje poznaje svoje korisnike, to algoritam može bolje pomoći oglašivačima da svoje proizvode predstave upravo ljudima za koje postoji veća vjerovatnoća da će im se svidjeti i da će ih kupiti. Ujedno, ovo im omogućava da svoje oglase personalizuju na način da različitim ljudima, s različitim interesovanjima, prikažu različite poruke, što za kompaniju predstavlja veliku vrijednost.

Vratimo se pitanjima koja smo postavili na početku ovog poglavlja. Vjerujemo da vaši odgovori govore o tome koliko su ove platforme postale uspješne u prepoznavanju onoga što nam se sviđa i onoga za čim baš u ovom trenutku tragamo.



Izvor: https://business.instagram.com/advertising/

Kao što možete vidjeti na slici iznad, ovo su neki od načina i podešavanja koje kompanije mogu odabrati prilikom odabira publike kojoj će biti prikazan njihov oglas. Ovdje je bitno napomenuti da kompanija nema pristup pojedinačnim podacima korisnika platforme, već zbirnim. Drugim riječima, Instagram služi kao svojevrsni posrednik između oglašivača i korisnika.

Na primjer, kao predstavnik kompanije koja prodaje najnoviji model patika za trčanje, razmisliću ko je obično publika koja nosi takve patike, a onda ću pokušati da nađem tu publiku na Instagramu. Osim lokacije (Crna Gora), demografskih podataka (recimo, muškarci i žene od 25 do 45 godina), pokušaću da dodatno personalizujem svoju publiku tako što ću tražiti ljude koji se inače bave trčanjem ili su zainteresovani za trčanje i učešće na maratonima, a koji će vrlo vjerovatno biti zainteresovani za proizvod koji nudim. Ukoliko zaista unesem sve te podatke u Fejsbukovu platformu za oglašavanje, koja služi i za Instagram, saznaću da u Crnoj Gori ima oko 35.000 takvih osoba i moj oglas će biti prikazan baš njima.

I to je dobitna kombinacija - kompanija uspije da proda svoje proizvode i održi se u životu, a maratonci dobiju najnoviju, još udobniju, sportsku opremu.

A šta je s onom majicom koja me prati svuda po internetu?

Često se desi da proizvod koji gledamo na nekom veb-sajtu kasnije nastavi da nas „prati" kuda god se kretali. To se zove ***retargeting* — proces u kojem korisnike koji su već došli na vaš veb-sajt i pokazali interes za neki vaš proizvod ili uslugu, targetirate posebnim oglasima čiji je cilj da korisnika vrate na veb-sajt i navedu ga da završi kupovinu.**

Izvor: https://marketingland.com/every-marketer-leverage-retargeting-96352

Kompanija ne prati nas lično, niti zaista zna šta radimo i gdje se nalazimo u trenutku u kojem nam prikazuje svoj oglas. Naime, proces funkcioniše tako što kompanija postavi poseban dio koda na svoj veb-sajt. Svaki put kad posjetimo taj veb-sajt, ili posebnu stranicu veb-sajta, postavljeni kod automatski aktivira anonimni „kolačić" u našem pretraživaču, koji bilježi podatak da smo posjetili veb-sajt, da smo iskazali interes za određeni proizvod i slično. Kasnije, dok se krećemo internetom, taj kolačić „nosi" pomenute informacije, pa kad se nađemo na platformi za oglašavanje (kao što su društvene mreže ili Gugl oglasi), šalje se signal da platforma treba da nam plasira taj posebno dizajnirani oglas.

S aspekta marketinga, ovaj način oglašavanja je izuzetno efikasan jer se kompanija obraća korisnicima koji su upoznati s onim što ona nudi, a nekad je potrebno samo da nas neko malo „pogura" pa da se odlučimo da kupimo određeni proizvod ili uslugu. To je razlog zašto prilikom posjeta sajtovima često vidimo obavještenje o kolačićima. Sljedeći put kad vam se ukaže obavještenje tog tipa, pročitajte ga, vidite o čemu se radi.

Zašto je važno da sve ovo znamo?

Prije svega, ako želimo da budemo digitalni građani, izuzetno je značajno da znamo kako digitalni svijet funkcioniše. Bitno je da znamo koliko podataka različiti internet servisi imaju o nama i na koji način se ti podaci koriste. Za početak, ukoliko koristite bilo koji od Gugl alata, kao što su Džimejl, Jutjub i slično, preporučujemo vam da u podešavanjima vašeg profila pogledate šta to Gugl zna o vama i na osnovu čega vam plasira oglase koje vidite. Ukoliko želite, možete i da deaktivirate neke opcije praćenja. Na isti način možete provjeriti i kako vas Fejsbuk vidi (idite na 'Podešavanja' pa na 'Oglase') i preuzeti kontrolu nad vašim podacima koje ova kompanija prati, obrađuje i čuva.

S druge strane, nadamo se da shvatate da **vaš telefon nema potrebu da vas prisluškuje da bi znao šta želite ili šta vas interesuje.** Korisnički profili koje servisi koje svakodnevno koristimo kreiraju o nama toliko su usavršeni da s velikom tačnošću to mogu sami da predvide. Ne radi se, dakle, o tome da negdje u Kaliforniji, u nekom zamračenom sobičku sjedi osoba koja se bavi internet tehnologijama i koja proučava naše podatke. Ne. To sve radi **kompjuter, koji se bavi obradom velikog broja podataka u isto vrijeme, a poređenjem našeg ponašanja na interenetu s ponašanjem ostalih korisnika izvodi određene zaključke.** Zaključke koji su najčešće tačni.

Postoji mnogo prednosti ovakvog razvoja tehnologije. Na primjer, veliki broj ljudi će vam reći da im je apsolutno OK da Amazon analizira njihove čitalačke navike ako to znači da će im svaki put dati dobru preporuku ili ih obavjestiti kad izađe najnovija knjiga njihovog omiljenog autora/autorke. Isti je slučaj i s preporukama sa Asosa i sličnih platformi. Ono što je važno jeste da sve vrijeme budemo svjesni šta se dešava, kako bismo reagovali u momentu kad to prestane da nam bude OK.

Naravno, razvoj digitalnih tehnologija nosi i veliki broj nedostataka. Sjetimo se slučajeva u kojima baze podataka bivaju napadnute i podijeljene bez dozvole, ili u kojima podaci bivaju zloupotrijebljeni i iskorišćeni za manipulisanje javnim mnjenjem kao što je to bilo u slučaju Kembridž analitike.

Korisnički podaci su valuta interneta i ono što podstiče cio sistem. Njihova vrijednost je ogromna, te je vrijeme da i mi kao korisnici, a pogotovo kao oni koji će tek imati uticaj na način na koji internet funkcioniše, budemo svjesni toga.

Da rezimiramo: svi mi jesmo (i moramo biti) digitalni građani. Kao takvi, neophodno je da se konstantno edukujemo i istražujemo što više možemo o dobrim, ali i o lošim stranama korišćenja interneta i digitalnih tehnologija, kako bismo zaštitili sebe i ljude oko nas.

Teme koje je ova elektronska knjižica pokrila izuzetno su bitne uvijek i svuda, a posebno u vremenu pandemije, kad smo prinuđeni da većinu aktivnosti izmjestimo u onlajn svijet. Nadamo se da vam je ovaj priručnik pomogao da bolje razumijete značaj digitalnog otiska, bezbjednosti na internetu, kao i da ste zapamtili neke od ključnih savjeta za prepoznavanje onlajn prevara, zaštitu ličnih podataka i balansiranu upotrebu tehnologije. Za kraj smo ostavili jednu lijepu priču o digitalizaciji i ulozi škola u stvaranju digitalno pismenog društva.

U kom stepenu su učenici u školama širom Crne Gore spremni da koriste digitalne tehnologije u procesu nastave i učenja?

Digitalna kompetencija predstavlja odlučnu, sigurnu i odgovornu upotrebu digitalnih tehnologija i njihovo pravilno i efikasno korišćenje za učenje, rad i učestvovanje u društvu. Ona uključuje informatičku pismenost, komunikaciju i saradnju, medijsku pismenost, stvaranje digitalnih sadržaja (uključujući programiranje), sigurnost (uključujući digitalnu dobrobit i kompetencije povezane sa sajber bezbjednošću), pitanja povezana s intelektualnim vlasništvom, rješavanje problema i kritičko razmišljanje.

U obrazovnom sistemu Crne Gore digitalna pismenost se razvija prvenstveno kroz obavezne i izborne nastavne predmete, ali i kroz ogroman broj nastavnih aktivnosti koje se realizuju korišćenjem digitalnih tehnologija u procesu nastave i učenja. Da bi se unaprijedilo i podržalo razvijanje digitalnih kompetencija, povećao kvalitet nastave i učenja i podigao nivo postignuća učenika, urađen je Okvir digitalnih kompetencija za sve nivoe douniverzitetskog obrazovanja.

Od ove školske godine, u svim osnovnim školama koristiće se i digitalni udžbenici za učenike prvih razreda koji će višestruko osavremeniti proces nastave i učenja. Obezbjeđivanje dobre internet konekcije u svakoj školi i nabavka informatičke opreme u značajnoj mjeri doprinosi digitalnoj pismenosti i nastavnika i učenika. U našoj zemlji je u posljednjih pola godine, kroz proces realizacije nastave na daljinu, znatno unaprijeđena didaktička pismenost nastavnika i učenika. Posebno je važno što su učenici uvidjeli koliki je značaj upotrebe digitalne tehnologije u procesu nastave i učenja.

Da li upotreba digitalnih tehnologija u sistemu obrazovanja može umanjiti problem nedostatka funkcionalnog znanja (povezivanje gradiva iz različitih oblasti i nadograđivanje postojećih znanja)?

Digitalne tehnologije su najveći globalni pokretač inovacija, konkurentnosti i privrednog rasta. One već utiču na sve aspekte života, tako da će sigurno činiti nezamjenjiv dio svijeta u kojem će današnja djeca živjeti i raditi. Izazovi i potencijali digitalnog obrazovanja su mnogostruki. Upotreba digitalnih tehnologija u procesu nastave i učenja utiče na motivaciju učenika i ima pozitivne efekte na njihova postignuća ukoliko se koristi na odgovarajući način, odnosno kad dopunjava postojeće nastavne pristupe. Uključivanje digitalnih tehnologija u glavne principe podučavanja i učenja omogućava inovaciju i unapređuje kompetencije, kao što su kritičko mišljenje, rješavanje problema i timski rad, pa je očekivano da će unaprijediti i funkcionalno znanje učenika.

Da li upotreba digitalnih tehnologija u sistemu obrazovanja može umanjiti problem nedostatka funkcionalnog znanja (povezivanje gradiva iz različitih oblasti i nadograđivanje postojećih znanja)?

Digitalne tehnologije su najveći globalni pokretač inovacija, konkurentnosti i privrednog rasta. One već utiču na sve aspekte života, tako da će sigurno činiti nezamjenjiv dio svijeta u kojem će današnja djeca živjeti i raditi. Izazovi i potencijali digitalnog obrazovanja su mnogostruki. **Upotreba digitalnih tehnologija u procesu nastave i učenja utiče na motivaciju učenika i ima pozitivne efekte na njihova postignuća ukoliko se koristi na odgovarajući način, odnosno kad dopunjava postojeće nastavne pristupe.** Uključivanje digitalnih tehnologija u glavne principe podučavanja i učenja omogućava inovaciju i unapređuje kompetencije, kao što su kritičko mišljenje, rješavanje problema i timski rad, pa je očekivano da će unaprijediti i funkcionalno znanje učenika.

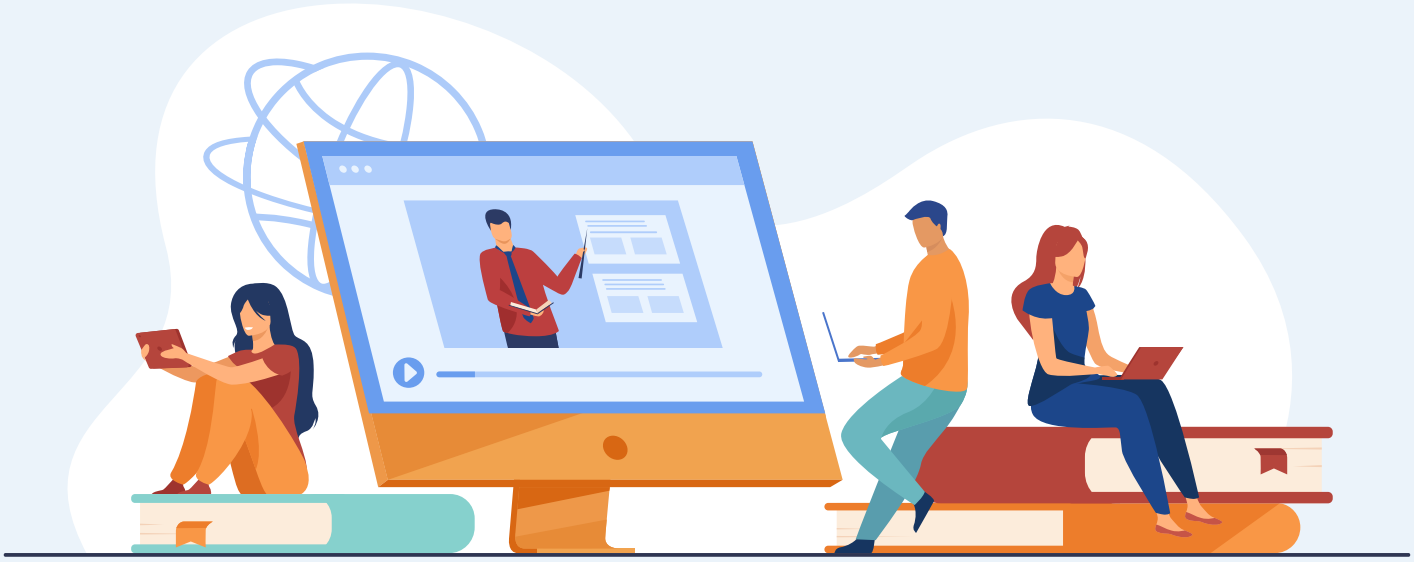
Koji su glavni ciljevi Okvira digitalnih kompetencija?

Osnovni cilj implementacije Okvira digitalnih kompetencija jeste stvaranje digitalno pismenog društva. Da bismo postigli, kroz proces obrazovanja je neophodno omogućiti:

- razvijanje sigurne, kritičke i odgovorne upotrebe digitalnih tehnologija u svim segmentima (učenje, rad, socijalne interakcije....);
- podizanje na viši nivo informatičke i digitalne pismenosti;
- unapređivanje komunikacije i saradnje;
- stvaranje digitalnih sadržaja (uključujući i programiranje);
- podizanje svijesti o značaju bezbjednosti (uključujući digitalnu dobrobit i kompetencije povezane sa sigurnošću);
- produbljivanje znanja u vezi sa intelektualnom svojinom;
- rješavanje postojećih problema.

Digitalna kompetencija – uticaj na podizanje svijesti o zaštiti ličnih podataka na internetu i o etičkom korišćenju digitalnih tehnologija

Digitalna kompetencija obuhvata pet oblasti: informaciona i digitalna pismenost, komunikacija i saradnja, kreiranje digitalnog sadržaja, bezbjednost i rješavanje problema. Ove oblasti su međusobno povezane i nadograđuju se jedna na drugu kako bi osigurale sistemski razvoj opšte digitalne pismenosti adolescenata i mladih. Oblasti se jednostavno mogu povezati s nastavnim sadržajima različitih predmeta/modula. U nekim se djelovima preklapaju, ali svaka oblast digitalne kompetencije ima svoje specifičnosti i utiče na razvoj posebnih znanja, vještina i stavova.



Ishodi učenja koji se realizuju kroz oblast bezbjednosti direktno upućuju na značaj zaštite ličnih podataka na internetu, ali i etičkog korišćenja digitalnih tehnologija. Izučavanjem ove oblasti učenici razvijaju kompetencije koje se odnose na zaštitu uređaja i digitalnog sadržaja, razumijevanje rizika i prijetnji u digitalnom okruženju, korišćenje sigurnosnih i zaštitnih mjera i pouzdanost i privatnost.

Oni takođe razvijaju kompetencije koje će im omogućiti da zaštite lične podatke i privatnost u digitalnom okruženju, primjenjuju specifične načine zaštite zdravlja i dobrobiti, te da koriste digitalne sadržaje u zaštiti životne sredine.

Adekvatna primjena digitalne kompetencije u obrazovnom sistemu

Digitalna kompetencija je sastavni dio obrazovnog programa, pa njena uspješna primjena podrazumijeva ocjenjivanje/procjenjivanje učeničkih postignuća.

Procjena i evaluacija multidisciplinarnih kompetencija učenika kompleksniji je zadatak nego procjena kompetencija koje se odnose na jednu disciplinu. Efikasna procjena pomaže učenicima da napreduju i doprinosi kvalitetu podučavanja i učenja. Veoma je važno da se odvija na više nivoa, s kriterijumima koji se kreću od usvajanja znanja, razvijanja vještina i uvažavanja različitih stanovišta, do naprednog nivoa ovladavanja digitalnom kompetencijom. Takvo praćenje, vrednovanje i ocjenjivanje predstavlja složen proces. **Svaka od oblasti digitalne kompetencije ogleda se u kriterijumima ocjenjivanja.** Strategije za procjenu treba da obuhvate kompleksnost znanja, vještina i stavova koji se stiču kroz multidisciplinarni pristup.

Cilj Okvira digitalnih kompetencija jeste digitalno opismenjavanje svih mladih i adolescenata u Crnoj Gori. Značaj digitalne pismenosti svima poznat od ranije, pandemija COVID-a-19 nas je suočila sa situacijama da postoje situacije u kojima vještina korišćenja digitalnih tehnologija postaje uslov kako za opstanak, tako i za bilo kakav napredak.

Iako nam je Prva pomisao na upotrebu interneta (i svih dostupnih digitalnih tehnologija) gotovo uvijek je zabava, no važno je prepoznati i više ciljeve. Ono čemu treba da težimo jeste školski sistem koji može da obezbijedi digitalno obrazovanje za sve i da nas, kroz niz zabavnih i edukativnih sadržaja, upozna s beskonačnim mogućnostima koje digitalne tehnologije pružaju.

Sajtovi za provjeru relevantnosti informacija:

Snopes: snopes.com
PolitiFact: politifact.com
Fact Check: factcheck.org
BBC Reality Check: bbc.com/news/reality-check
Channel 4 Fact Check: channel4.com/news/factcheck
Reverse image search from Google: google.com/reverse-image-search

SOS linija za prijavu nasilja: 080 777 777

Sajt za prijavu onlajn prevare: http://www.cirt.me/cirt

U okviru projekta „Bezbjednost na internetu u doba pandemije COVID-a-19", koji realizuje Digitalizuj.Me, uz podršku UNICEF-a i Telenora, kreiran je niz od 10 edukativnih blog-postova, koji čine ovu elektronsku knjigu.

Imajući u vidu da se sve više društvenih aktivnosti seli u onlajn okruženje, projekat „Bezbjednost na internetu u doba pandemije COVID-a-19" osmišljen je s ciljem da kroz niz edukativnih programa i sadržaja podigne svijest adolescenata o rizicima na internetu i pruži im znanja i vještine neophodne za sigurno korišćenje tehnologije.

U okviru projekta održano je pet edukativnih radionica:

- „Šta znači „privatno" na internetu?", predavačica - Sanja Gardašević, projektna menadžerka u Digitalizuj.Me i izvršna direktorica digitalne marketinške agencije Alicorn
- „Kako se zaštiti od onlajn prevara?", predavač - Milutin Pavićević, član Digitalizuj.Me tima i izvršni direktor u kompaniji ME-net, najvećem crnogorskom veb hosting provajderu
- „Onlajn i oflajn stilovi komuniciranja – kako prevazići komunikacijiski šum i stvoriti bezjedno onlajn okruženje", predavačica - Danijela Knežević, suosnivačica agencije Memento marketing i komunikacije i menadžerka kreativnih komunikacija u toj agenciji
- „Balansirana upotreba tehnologije", predavačica - Nataša Đukanović, direktorica marketinga u kompaniji DoMEn, registraru crnogorskog nacionalnog domena .ME
- „Lažne vijesti", predavačica - Jelena Jelušić, doktorandica i asistentica na Katedri za radio, televiziju i film na Univerzitetu Nortvestern u Čikagu

U okviru projekta kreirano je i sedam edukativnih videa:

1. Bezbjednost na internetu u doba pandemije - prvi dio
2. Bezbjednost na internetu u doba pandemije - drugi dio
3. Bezbjednost na internetu u doba pandemije - treći dio
4. Bezbjednost na internetu u doba pandemije - četvrti dio
5. Bezbjednost na internetu u doba pandemije - peti dio
6. Bezbjednost na internetu u doba pandemije - šesti dio
7. Bezbjednost na internetu u doba pandemije - sedmi dio

Glumci: Aleksandra Šovran, Anastasija Šovran, David Vuković i Ivana Popović


telenor


DIGITALIZUJ.ME


unicef
za svako dijete