Digitalni identitet

Petrović, Jan

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

JAN PETROVIĆ

DIGITALNI IDENTITET

Diplomski rad

Pula, 2018.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

JAN PETROVIĆ

DIGITALNI IDENTITET

Diplomski rad

Broj indeksa: 468-ED

Studijski smjer: Poslovna informatika

Mentor: Prof. dr. sc. Mario Radovan

Pula, veljača 2018.

Sadržaj

Popis slika

1. UVOD

Računalna tehnologija jedan je od najinteresantnijih ljudskih izuma[1], koja je gotovo od svog nastanka omogućavala ljudima da međusobno komuniciraju, te je kroz desetljeća i godine razvijana da na nove, bolje i brže načine pomogne u komunikaciji, načine koji bi bili nemogući da ista ne postoji. Omogućila je ljudima da vide i čuju dalje negoli su im to omogućavale oči i uši, omogućila im je da promatraju i vide događaje koji se odvijaju tisućama kilometara daleko, u dubinama oceana, vrhovima najviših planina, omogućila im je da vide svijet u kojem žive iz svemira, da vide površinu Mjeseca, da otkriju svijet oko sebe.

No informatička tehnologija ne omogućava samo komunikaciju ili prijenos događaja iz okoline – informatička tehnologija sve više stvara tu okolinu u kojoj živimo ili s kojom komuniciramo. Unatrag nekoliko desetljeća, pa sve do pred nekoliko godina, ljudi su prihvaćali stvarnost koja im je nuđena , ona koju su mediji poput televizije ili radija prenosili publici, a na koju ljudi – potrošači iste – nisu mogli utjecati. Napredovanjem tehnologije i to je prestao biti problem, sada upravo korisnici stvaraju svoju okolinu, onu virtualnu, u kojoj borave putem informatičko-komunikacijskih kanala, a koja im sve više i više pažnje oduzima, čineći tu virtualnu okolinu gotovo pa pravom. Nije to nekakva novost 21. stoljeća, ljudi su odavno pokušavali makar na kratko, pobjeći u virtualnu stvarnost, putem knjiga, crteža, i ostalih oblika stvaralaštva.

Stvarnost, realna okolina, ne pruža ljudima onoliko slobode koliko bi oni željeli, a niti se ne prilagođava svim njihovim željama, dapače – često je surova i frustrirajuća. Ljudi su često stvarali sebi prihvatljivu , ugodnu alternativnu virtualnu stvarnost, kako bi u nju mogli pobjeći od one realne. Kroz stoljeća se promijenila ta vrsta virtualne stvarnosti, međutim u novije doba informatičko-komunikacijska tehnologija omogućava da se virtualna stvarnost prilagodi, do određene mjere, svakom korisniku. ovdje je sada bitno spomenuti pojam interneta, kao globalne komunikacijske mreže sa svim popratnim sadržajem, a koje je glavni razlog postojanja globalno povezanih oblika virtualne stvarnosti koje su zadnjih godina poprimile veliku važnost – društvenih mreža i društvenih zajednica. Kako bi se omogućilo ljudima korištenje i realnih usluga u toj virtualnoj stvarnosti, stvorene su i razne usluge koje su povezane sa realnim uslugama koje građani koriste posredstvom interneta. Stoga, internet svojim korisnicima nudi povezanost sa virtualnim svijetom, kojeg korisnici koriste kako žele, kao i povezanost sa realnim svijetom i realnim uslugama, no uz komociju udaljenog, može se reći digitalnog pristupa, ili izvršenja, konzumiranja, takvih usluga. O svemu tome, biti će riječi u nastavku ovog rada.

1 Radovan, Mario (2016). "Communication and Control: The shaping of reality and people"

2. RAČUNALNE MREŽE

Računalna mreža omogućava komunikaciju međusobno povezanih računala. Da bi se formirala računalna mreža, potrebna su najmanje dva uređaja povezana bakrenim ili optičkim kabelom, ili bežično – preko njih se razmjenjuju podaci i dijele resursi. Lokalne računalne mreže (engl. LAN – Local Area Network) povezuju računala i opremu na manjem geografskom području, poput jedne ili više zgrada. Komunikacija između računala i uređaja na širem geografskom području se ostvaruje vezivanjem na lokalnih mreža na veću mrežu – WAN mrežu (engl. WAN – Wide Area Network), poput Interneta.

Mrežni zadaci podijeljeni su u referentnom modelu OSI (engl. OSI - Open Systems Interconnection) na sedam manjih, lakše upravljanih slojeva, od kojih svaki definira određene funkcije mreže. Prednost upotrebe OSI modela su jednostavnost, standardizacija, sprečavanje utjecaja promjene na jednom sloju na druge slojeve, te lakši izbor pravog mrežnog uređaja za određenu namjenu. Funkcije slojeva su slijedeće: [2]

- Fizički sloj – prijenos bitova
- Podatkovni sloj – razmjena podataka između mrežnih uređaja, detekcija i korekcija potencijalnih grešaka na fizičkom sloju
- Mrežni sloj – logičko adresiranje i usmjeravanje (rutiranje)
- Transportni sloj – logička veza s kraja na kraj i kontrola toka
- Sloj sesije – uspostava veze između računala i sinkronizacija iste
- Prezentacijski sloj – formiranje podataka
- Aplikacijski sloj – pristup aplikacije mrežnom okruženju

Ukoliko sustavi nisu direktno međusobno povezani, koriste se posredni mrežni uređaji koji implementiraju niže slojeve OSI modela. U zavisnosti od slojeva koji su implementirani, za te uređaje će biti važni bitovi, okviri (engl. frames) i paketi (engl. packets). To određuje funkciju uređaja: fizički sloj – koncentrator (engl. hub) , podatkovni sloj – preklopnik (engl. switch), mrežni sloj – usmjeravatelj (engl. router). S obzirom da nema nikakve modifikacije podataka iz viših slojeva, postojanje ovakvih uređaja u mrežnoj infrastrukturi je za korisnika transparentno.

2 Radovan Mario , (2011). “Računalne mreže 2”

2.1. Skup protokola TCP/IP

Skup protokola TCP/IP razvila je američka sigurnosna agencija DARPA, te je nedugo zatim implementiran u prvu svjetsku mrežu – ARPANET, tokom 70ih godina prošlog stoljeća. Danas se na tim protokolima bazira komunikacija na Internetu, te su oni postali standard za povezivanje računala i mreža. TCP/IP model čini nekoliko slojeva: sloj pristpa mreži, Internet sloj, transportni sloj i aplikacijski sloj. Internet sloj odgovara mrežnom sloju u OSI modelu, a bavi se adresiranjem i usmjeravanjem paketa, čime osigurava vezu između računala koji se ne moraju nalaziti fizički na istoj mreži. Na ovom se sloju koriste slijedeći protokoli:[3]

- IP (engl. Internet Protocol) – osnovni protokol koji osigurava prijenos informacija od računala do računala
- ICMP (engl. Internet Control Message Protocol) – IP protokolu osigurava kontrolne poruke o greškama, te se najčešće koristi za provjeru dostupnosti ciljnog računala
- ARP (engl. Address Resolution Protocol) – Osim IP adrese, svaki mrežni uređaj ima svoju fizičku adresu (MAC adresu) koja bi trebala biti unikatna svakom pojedinom mrežnom uređaju, te ih dodjeljuje proizvođač. One se koriste prilikom prijenosa *frame-a* podatka po fizički istoj mreži. ARP protokol prevodi IP adrese u MAC adrese.

Transportni sloj preuzima podatke s viših slojeva, po potrebi ih segmentira i uspostavlja virtualne veze te prenosi podatke do odredišta koristeći usluge Internet sloja. Na ovom sloju se koriste:

- TCP (engl. Transmission Control Protocol) – protokol koji garantira pouzdanu vezu i osigurava isporuku podataka u kontroliranom redoslijedu od pošiljatelja prema primatelju, te otkriva i ispravlja greške u prijenosu.
- UDP (engl. User Datagram Protocol) – protokol koji koristi jednostavan i minimalistički mehanizam prijenosa podataka, ne uspostavlja virtualne veze niti osigurava mehanizam za detekciju pogrešaka.

Aplikacijski sloj omogućava da aplikacije, odnosno korisnici, pristupe servisima Internet mreže. Česti protokoli koji se koriste su:

- HTTP (engl. HyperText Transport Protocol) – pristup Web stranicama

3 https://www.garykessler.net/library/tcpip.html#evol

- HTTPS (engl. HTTP Secure) – osigurani pristup Web stranicama
- FTP (engl. File Transfer Protocol) – prijenos datoteka
- POP3 (engl Post Office Protocol v3) – dolazna e-mail pošta
- SMTP (engl. Simple Mail Transport Protocol) – odlazna e-mail pošta
- DNS (engl. Domain Name System) – prevođenje tekstualnih adresa u IP adrese

2.2. IP adresiranje

Svako računalo i *router* na Internetu ima svoju jedinstvenu IP adresu (ili više IP adresa). IP adrese su 32-bitne, sastoje se od 4 okteta i uobičajeno se predstavljaju u decimalnoj notaciji s točkom (npr. 192.168.1.1). Ovaj sistem adresiranja je danas u upotrebi i naziva se još i IPv4 (engl. Internet Protocol version 4), no budući da broj istodobno povezanih računala svakim danom sve više raste, broj slobodnih IP adresa se rapidno smanjuje, te kako bi se spriječila situacija kada više neće biti slobodnih IP adresa, zadnjih godina se krenulo u implementaciju novog IP protokola, IPv6, koji se sastoji od 128-bitne adrese. Primjer IPv6 bi bio: 2001:db8:0:1234:0:567:8:1

Svaka IP adresa ima dva dijela – jedan je adresa IP mreže i ista je za sva računala i opremu u jednoj IP mreži, a drugi dio je adresa računala, jedinstvena za svako računalo u mreži. Na osnovi broja okteta koji pripadaju adresi mreže, odnosno adresi računala, IP adrese se dijele u klase A, B, C i D

Raspodjela IP adresa po blokovima je kako slijedi:

Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255

IP adrese se dalje dijele na javne i privatne. Javne adrese dodijeljuju RIR (engl. Regional Internet Registry) organizacije. U Europi za dodijeljivanje javnih adresa je nadležan RIPE NCC (Réseaux IP Européens Network Coordination Centre). Privatne adrese su namijenjene mrežama koje nisu direktno povezane na Internet i ne mogu se koristiti na Internetu. U njih spadaju:

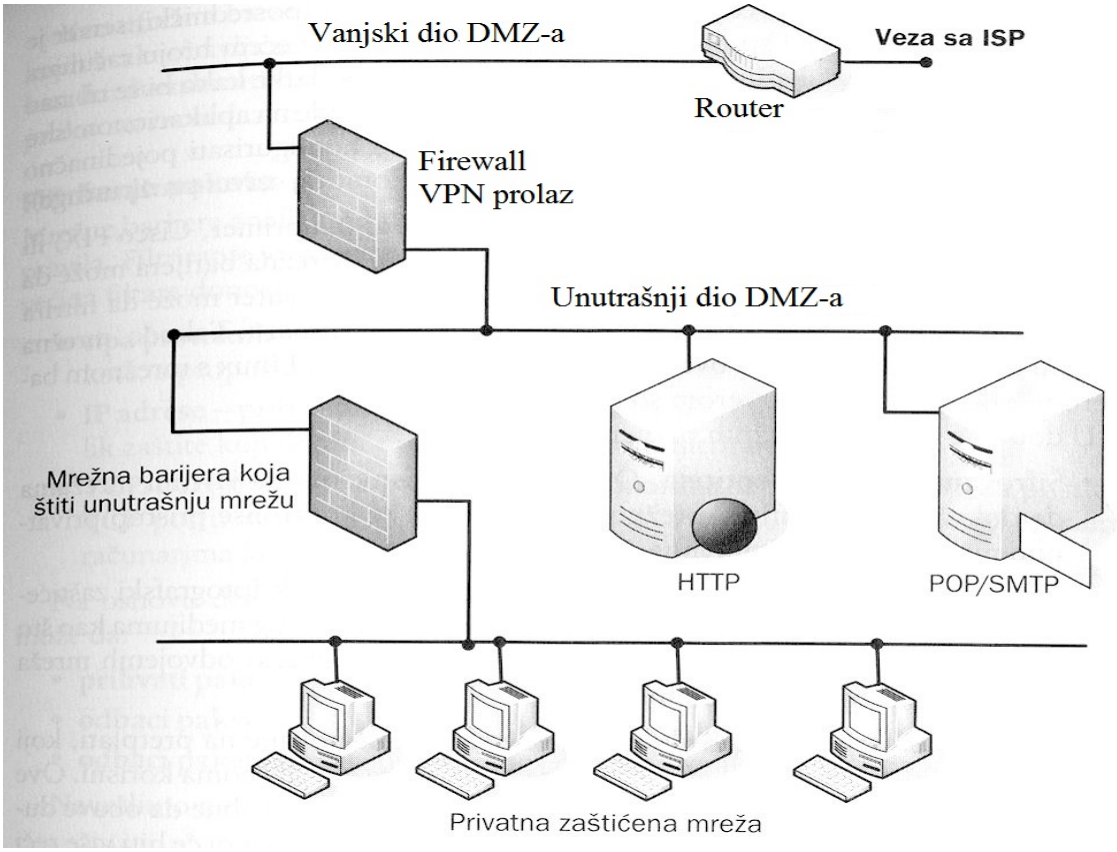
Početak:	Kraj:	Broj IP adresa:
10.0.0.0	10.255.255.255	16777216
172.16.0.0	172.31.255.255	1048576
192.168.0.0	192.168.255.255	65536

Maska podmreže (engl. Subnet mask) je 32-bitni broj nalik na IP adresu, koja determinira kojoj podmreži (engl. Subnet) neka IP adresa pripada. Maske podmreža u klasama A, B i C su redom: 255.0.0.0, 255.255.0.0 i 255.255.255.0. Adresa mreže se uvijek navodi s maskom podmreže. Na primjer, adresa mreže 192.168.10.0 u klasi C se zapisuje kao 192.168.10.0 255.255.255.0 ili 192.168.10.1/16, pri čemu broj 16 označava broj bitova koji pripadaju adresi mreže.
Subnet-ovi su segmenti iste IP mreže koje komuniciraju preko routera. Korištenjem *subnet*-ova se smanjuje broj računala na segmentima IP mreža s velikim brojem računala. Prednosti mogu biti razne – korištenjem subnetova može se rasteretiti routere te ubrzati brzinu protoka podataka, ili može pojednostaviti administriranje mreže. Osim toga, komunikacija između subnetova nije direktno moguća, te se moraju koristiti routeri, koji omogućavaju limitiranje komunikacije i blokiranje iste po određenim portovima.

Osim IP adrese, protokoli koriste i broj porta, koji omogućavaju uspostavljanje više istovremenih veza prema jednom računalu (tj. prema istoj ciljnoj IP adresi). Ukupno ima 2^{16} portova (0-65536). Servisi pokrenuti na nekom računalu osluškuju zahtjeve na određenim portovima, najčešće na rezerviranim portovima (0-1023) te za komunikaciju koriste TCP, UDP ili oba navedena protokola. Administratori mogu po potrebi zatvoriti određeni port, čime se onemogućava uspostavljanje veze i komunikacija prema nekom servisu.

2.3. Vatrozid

Vatrozid (engl. firewall) se koriste za postavljanje kontrolnih sigurnosnih točaka na granicama privatnih mreža. Tokom rada, *firewall* ispituje sve pakete koji prolaze između privatne mreže i vanjske mreže (Interneta). Ovisno o tome zadovoljava li paket podatka pravila definirana u konfiguracijskoj skripti, *firewall* će dozvoliti i blokirati prolaz tog paketa. Pojednostavljeno, *firewall* je filtar na relaciji lokalna mreža – Internet.



Slika 1: Grafički prikaz mreže sa firewall-om. Izvor: knjiga "Računalne mreže"

Funkcije koje *firewall* obavlja su najčešće: [4]

- Filtriranje paketa – analizira se zaglavlje (engl. header) paketa (u kojemu su zapisane početna i ciljna IP adresa, i broj porta) i uspoređuje sa sigurnosnim pravilima *firewall-a*. Ovisno o tome dali paket zadovoljava pravila, dozvoljava se prolaz paketa ili se isti odbacuje
- Prevođenje mrežnih adrasa (engl. Network Address Translation -NAT) – prevodi adrese računala u privatnoj mreži u jednu ili više javnih IP adresa, na taj način sakrivajući identitet i broj računala u lokalnoj mreži
- Kriptirana provjera identiteta – omogućava korisnicima koji pristupaju privatnoj mreži sa vanjske mreže da dokažu svoj identitet kako bi pristupili privatnoj mreži
- Virtualno privatno umrežavanje (engl. VPN) – uspostavljanje kriptirane veze između dvije privatne mreže preko javne mreže (poput Interneta). Time se osigurava sigurna veza između dvije fizički odvojene privatne mreže.

4 Pleskonjić i ostali (2007), "Sigurnost računarskih sistema i mreža"

- Antivirusna zaštita – analiziraju se paketi koji prolaze *firewall-om* te se pretražuju za postojanje virusa, crva, i ostalih zlonamjernih programa.
- Filtriranje sadržaja (engl. content filtering) – blokira se pristup web adresama i destinacijama koje su unesene u filtar listu kao nepoželjne (npr. pornografske stranice, video *streaming* itd).

2.4. Bežične (WI-FI) mreže

Tehnološkim napretkom te razvijanjem prijenosnih računala i ostalih mobilnih uređaja, nastala je potreba za povezivošću bez upotrebe kabela. Tokom 90ih godina 20. stoljeća ubrzao se razvoj i standardizacija uređaja koji koriste radio opseg za digitalnu dvosmjernu bežičnu komunikaciju, koji je potom zakonski određen – razvijen je IEEE 802.11 standard, bolje poznat kao *Wi-Fi*.

Radi se o standardu bežičnog povezivanja koji koristi zakonski dozvoljen frekvencijski spektar, što bi značilo da za njegovu upotrebu nije potrebno ishođenje dozvola (za usporedbu, GSM , radio, tv, i ostali frekvencijski opsezi se daju u koncesiju te se za njih plaća naknada za korištenje). Po standardu, postoje 2 frekvencijska opsega koji se na globalnoj razini koriste za *Wi-Fi* povezivanje , a to su 2.4 Ghz i 5 Ghz *band-ovi* . IEEE 802.11b, g i n standardi koriste frekvenciju od 2412 - 2472Mhz, unutar kojih se nalazi 13 kanala koji se koriste za komunikaciju, uz sitnije razlike ovisno o zakonskoj regulativi određenih zemalja. Ovo je najraširenij spektar kojega podržavaju svi bežični uređaji, te se globalno koristi za bežičnu komunikaciju. IEEE 802.11a standard je nastao paralelno sa prethodno spomenutim, no zbog određenih tehničkih problema kasnio je s izlaskom na tržište te je i danas slabije zastupljen, a velik broj uređaja ga i dalje ne podržava. Bitno je spomenuti da frekvencijski opseg kojega koristi jako varira od države do države, iako se koristi frekvencija od 4915mhz do 5825mhz, unutar čega postoji veći broj kanala koji se razlikuju po širini spektra, čime se regulira i njihova primjena, odnosno ograničava praktična primjena, pa se tako jedan dio opsega smije koristiti isključivo za internu upotrebu, drugom dijelu se limitira izlazna snaga, trećem dijelu opsega je smanjena širina spektra, itd. Jedna od prednosti korištenja ovog standarda je upravo njegova slabija zastupljenost, čime se omogućuje povezivanje na većim udaljenostima, s većim brzinama, manjim interferencijama uz sveukupnu veću pouzdanost. Kompanije koje su teritorijalno raširene ili imaju podružnice na područjima bez DTK

infrastrukture, korištenjem ovog standarda mogu rješiti svoje probleme s mrežnom povezanošću ukoliko već postoje bežične mreže na 2.4 ghz spektru.

Korištenje bežičnih mreža u poduzećima omogućava mrežno povezivanje prijenosnih računala i pametnih telefona na mrežnu infrastrukturu poduzeća, čime se zaposlenicima koji ovise o takvoj vezi omogućava rad, ali istovremeno omogućava zaposlenicima koji nemaju obavezno fiksno radno mjesto, da mijenjaju lokaciju te nastave rad na računalu nesmetano povezani, neovisno o tome što se ne nalaze u svom uredu. Da bi to bilo moguće, koriste se bežične pristupne točke (engl. Access Points – AP). Radi se o mrežnim uređajima koji se povezuju na postojeću mrežnu infrastrukturu kabelom, najčešće imaju još nekoliko utičnica za povezivanje računala i ostale opreme, te emitiraju bežičnu mrežu putem koje se korisnici mogu spojiti.

3. SIGURNOST KORIŠTENJA RAČUNALNIH MREŽA

Kada je riječ o Internetu, zna se da se radi o nesigurnoj mreži, doslovno se njegovim korištenjem dovodi u opasnost ne samo sigurnost računala, nego i vlastiti identitet, pa i vlastiti život. Već je prije bilo riječi o digitalnom identitetu, te o online identitetu. Koliko god korisnici ne razmišljali o opasnostima koje "vrebaju" na Internetu, one su stvarne, počevši od minornih i samo "neugodnih" susreta poput neke zloćudne ekstenzije u Internet browseru, koja korisnika maltretira sa reklamama i ponudama za kupnju raznih proizvoda, do onih ozbiljnijih koje prate ponašanje korisnika i pokušavaju ukrasti njegove osobne podatke. Oblika prevare ima puno, a trenutak nepažnje može dovesti do ozbiljnijih problema. Koliko god krađa online identiteta na nekoj društvenoj mreži , ili email računa zvučala ozbiljno, postoje drastično ozbiljniji problemi koje krađa online identiteta može prouzročiti. Ukoliko se korisnika preusmjeri na stranicu sličnu onoj kojoj želi pristupiti, što se može desiti prilikom pristupanja stranicama za internet bankarstvo, razna online plaćanja, ili uslugu e-građana, tvorac takvog programa (popularno nazvan hakerom) dobije sve što mu treba da ukrade nečiji digitalni identitet, time dobivajući mogućnosti da upravlja i stvarnim životom korisnika, trošeći njegova financijska sredstva, potpisujući u njegovo ime razne ugovore i tome slično. Danas kada je osnovni oblik identifikacije OIB, dovoljno je poznavanje nečijeg imena, prezimena i OIB-a da bi se otuđio identitet. Iako zvuči kao daleka budućnost iz nekog filma znanstvene fantastike, ovakve prijetnje su ne samo realne, nego se i događaju.

Ne ulazeći u samu sigurnost Interneta kao mreže, kao i kućne korisničke mreže što također može rezultirati kriminalnim radnjama, postoji nekoliko glavnih tipova prijetnji kojima su korisnici konstantno izloženi. Za neke od tih prijetnji postoje informatička rješenja koja ih neutraliziraju, no za neka druga jedino korisnička pažnja može pomoći:

- *Phishing* (pecanje, odnosno mrežna krađa identiteta)
- Internet prijevare
- Email prijevare
- Spyware/Malware/Virusi

U nastavku teksta biti će objašnjene svaka od navedenih prijetnji. Zajedničko svima jest da ciljaju na krađu korisničkog identiteta, a ovisno o tome što uspiju "ukrasti" korisniku mogu prouzročiti i poprilično veliku materijalnu štetu. 90Ih godina, koje se mogu smatrati ranom fazom interneta, takve prijetnje nisu bile od velikog značaja, a ujedno ih je bilo i manje, iz jednostavnog razloga što su pristup internetu tada imale pretežno kompanije, fokus hakera je bio na napadanju internih mreža velikih kompanija i krađi njihovih podataka. Malih korisnika interneta nije bilo ni približno brojem kao danas, pristup internetu je bio iznimno spor, a i sami korisnici nisu ostavljali svoje osobne podatke jer je broj usluga koje su se pružale bio relativno minoran. Danas korisnik na internetu praktički živi još jedan život, pruža mu se ogroman broj usluga koje se uzimaju zdravo za gotovo i o njima se gotovo i ne razmišlja kao o "usluzi" jer su se toliko udomaćile da ih se takvima ne percipira, poput instant poruka, emaila, internet bankarstva, online buking portala i slično, no u začecima interneta takvih usluga nije bilo, stoga se krađe identiteta i nisu mogle dogoditi. Danas, s druge strane, takve opasnosti vrebaju konstantno, te je bolje da se korisnici čim bolje upoznaju s njima, kako bi ih uspješno zaobilazili.

3.1. Phishing – mrežna krađa identiteta

Govoreći o *phishingu,* misli se na krađu identiteta pokušavajući zavarati korisnika da se radi o legitimnom upitu. Primjerice, korisnik dobije email čiji sadržaj izgleda poput onoga kojeg inače šalje banka, ili bilo koji drugi popularni servis, poput Paypala, Ebaya, Facebooka, i slično. U takvim je emailovima uvijek jedna poveznica koja, na prvi pogled, otvara zvaničnu stranicu, no "ispod" poveznice se krije druga stranica, na koju se korisnika prevarom pokušava natjerati. Jednom otvorena takva stranica, ona će estetski izgledati poput zvanične stranice, ili biti veoma slična njoj,

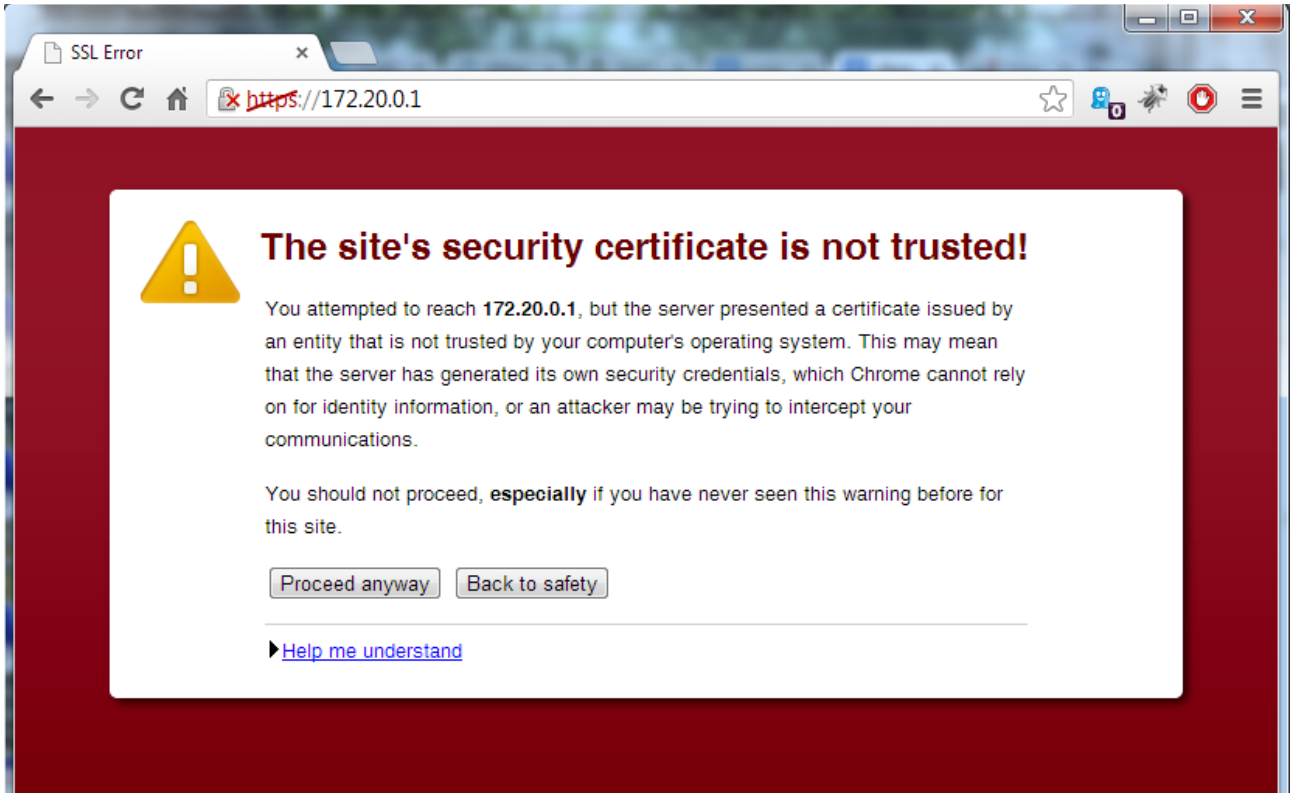
no razlikovati će se u linku koji je naveden u adresnoj traci. Dok je , na primjer, zvanična web adresa Paypal servisa www.paypal.com, korisnika će dočekati estetski identična stranica, samo što će njezina web adresa biti tek malo drugačija i možda teško uočljiva, poput www.paypol.com ili tome slično. Jednom kada se korisnik "spoji" sa svojim korisničkim podacima, njegov će online identitet biti ukraden, pružajući tvorcima stranice mogućnost da koriste novac na paypal računu ovako prevarenog korisnika. Sličan scenarij je moguć sa bankama, gdje će korisnik dobiti email u kojemu ga se traži "provjera ispravnosti" kreditne kartice, na način da upiše svoje osobne podatke , uključivo i broj kartica i tajni CSV broj, koji služi sa provjeru kartice. Ukoliko tvorac stranice dođe do takvih podataka, velika je vjerojatnost da će kroz samo par minuta vlasniku kartice biti ukradena veća svota novca. Sam akt phishinga se smatra socijalnim inženjerstvom, jer iako se radi o tehničkom napadu radi medija kojim se širi i na kojemu se njegov rad bazira, glavna komponenta tog akta je nesavjestan, ili neupućen korisnik koji svojevoljno pristaje biti meta napada. Na računalima se ovakva vrsta napada može djelomično previdjeti, iz razloga što se u email pregledniku vidi "mimificirani" link koji je zamaskiran, kao i zbog činjenice da se adresna traka u pretraživačima interneta vidi, dok na mobilnim uređajima i jedna i druga stavka nisu vidljive, ili su slabo vidljive, zbog načina na koji moderni pametni telefoni rade i prikazuju sadržaj.

Postoji i drugi način krađe identiteta, a to je telefonskim putem. U Hrvatskoj se ovakav način krađe događa rijetko, mada je bilo pokušaja kada su korisnici bili nazivani od strane "tehničke podrške" koja je "detektirala virus" na računalu korisnika i nudila da ga otkloni, dok bi zapravo od korisnika tražili da im dozvoli pristup računalu izvana.

3.2. Internet prijevare

Internet prijevara se odnosi na bilo koji čin prijevare na internetu, reklamiranjem nepostojećih proizvoda poput online prodaje ualznica, mobitela, i slično. Korisnik bi uplatio traženu svotu u uvjerenju da će mu proizvod biti isporučen, no ili mu se isporuči nešto bezvrijedno, ili mu se ne isporuči ništa. U odnosu na phishing, gdje se koriste lažne stranice, kod ovakvog tipa prijevare virtualni proizvod se može reklamirati i na pravim web trgovinama, poput ebaya, aliexpressa i slično. I iako se za navedenu prijavaru ne radi o krađi identiteta, svejedno dolazi do otuđenja novca. Usko povezano sa ovim tipom krađe jest prijevara gdje se korisniku kradu podaci o kartici, ili se prikazani iznos za naplatu razlikuje od iznosa koji će korisniku biti naplaćen. Kod ovakvog tipa prijevare, uz minimalnu pažnju može se spriječiti nemili događaj: moderni pretraživači interneta u

adresnoj traci zelenom bojom signaliziraju sigurnu stranicu i uspostavu sigurne veze (HTTPS), također ispišu i naziv certifikata kojeg stranica koristi i ako je on potvrđen – stranica je sigurna za "upotrebu" i online plaćanje. Za slučaj da se koristi HTTPS veza, ali stranica nema odgovarajući certifikat, korisniku će to biti vidljvo iz adresne trake u kojoj će crvenom bojom biti označena poveznica, uz obavijest da je certifikat istekao ili nepostojeći.



Slika 2: Primjer nesigurne veze, izvor: https://i.stack.imgur.com/myTwa.png

Razlog spominjanja internet prijevara je u tome što se korisniku ovim činom krade digitalni indentitet putem validnih portala, ili barem djelomično validnih (krađa može nastati prlikom preusmjeravanja na portal koji odrađuje plaćanja). No osim direktnih internet prijevara poput gore navedenih, vrlo bitna opasnost koju vrijedi spomenuti jesu razni nepoćudni programčići koji se instaliraju na računalo korisnika. Radi se o raznim spyware, malware i sličnim programčićima, štetnim ekstenzijama za internet preglednike, pa i virusima i trojancima kojima se zarazi računalo korisnika, a koji mogu pratiti aktivnosti koje korisnik obavlja na računalu, preusmjeravati korisnika na neželjene stranice, pratiti odnosno snimati tipkovnicu i ostalo. Ukoliko korisnik koristi zaštitu, ovakva vrsta prijetnji se može djelomično umanjiti, no sve je veći broj ovakvih aplikacija koje se predstavljaju kao legitiman softver, a korisnik samovoljno daje pristanak za njihovu instalaciju. To se događa često prilikom instalacije određenog traženog softvera koji u sklopu instalacije nudi i

“dodatak” , a neupućeni korisnik bez čitanja samo dozvoli instalaciju. Osim tog načina isntalacije, često se nepoćudni programi kriju iza reklama na web stranicama, a korisnik koji zabunom klikne na njih, nepažnjom dozvoli instalaciju nepoćudne ekstenzije u preglednik. Neke ekstenzije samo korisniku prikazuju reklame na web stranicama koje ih inače nemaju, dok su druge opasnije te korisnika preusmjeravaju na točno definirane portale, često “presjecajući” konekciju između dvije povezane stranice. Kao primjer se može uzeti postupak online plaćanja kupljene robe na nekom od poznatih portala za internet prodaju, gdje se nakon kupnje korisniku nudi unos podataka o kartici ili otvaranje paypal stranice u koju će korisnik unijeti svoje login podatke kako bi joj pristupio. U normalnim okolnostima otvoriti će se legitiman paypal prozor, korisnik će upisati svoje korisničke podatke, i potvrditi plaćanje. Kod preusmjerene stranice, može ga dočekati slična stranica samo što unosom korisničkih podataka ga neće dočekati potvrda o plaćanju, već vjerojatno nekakva greška, ili prozorom gdje ga se dodatno pitaju i podaci o kreditnoj kartici. Već u prvom koraku, a to je bio udnos korisničkih podataka, njegovi su podaci već ukradeni i tvorac stranice već ima pristup njegovom paypal računu, no ako je korisnik slabo informiran i nepažljiv, unosom podataka o kreditnoj kartici doslovno poklanja kreditnu karticu tvorcu stranice. Gašenje računala , što je inače instinktivna reakcija, neće se ništa postići, jer su podaci već poslani i ukradeni. Ovdje samo pažnja korisnika može pomoći. O tome da se ne radi samo o prijetnjama na stranim portalima, ukazuje i činjenica da su tokom 2014. godine slični napadi bili provođeni i na stranicama hrvatskih banaka, gdje se prilikom spajanja na sustav online plaćanja od korisnika tražio unos mac 2 koda sa svog tokena, a koji inače služi za autorizaciju i provedbu online platnih naloga.


otpbanka Građani - upute Poslovni subjekti - upute

Internet bankarstvo - važna obavijest

Savjeti za sigurno korištenje usluge Internet bankarstva

OTP banka posebnu pozornost posvećuje sigurnosti računa i osobnih podataka svojih klijenata u skladu s najvišim tehnološko-sigurnosnim standardima. Ovom obaviješću podsjećamo Vas na pravilno korištenje usluge eLEMENT@ Internet bankarstva, kako biste i Vi sami pridonijeli višoj razini sigurnosti.

Nikada nemojte:

- unositi podatke s tokena na ekrane koji izgledaju neuobičajeno (npr. prikazuje se brojač/poruka da je autentifikacija u tijeku), ili koji sadržavaju neobične poruke (ne sadržavaju hrvatske znakove, nisu pisani sukladno hrvatskim pravopisnim pravilima), ili ako je proces na ekranu usporen,
- provoditi autorizaciju / unositi podatke s tokena (serijski broj tokena, APPLI_) ni na kojem ekranu osim kad ste unutar eLEMENT@ Internet bankarstva,
- na zahtjev drugih osoba odavati PIN, podatke o tokenu ili druge povjerljive podatke koji su povezani s Vašim poslovanjem s Bankom, pristupati nepoznatim stranicama ili otvarati stranice s linkova dostavljenih u okviru sumnjive elektroničke pošte, kako ne biste zarazili svoje računalo.

Napominjemo da Vas zaposlenici Banke nikad neće tražiti odavanje povjerljivih podataka kao što su prethodno navedeni (PIN, token i slično), stoga molimo da ih nikad ne odajete trećim osobama putem telefona/e-maila/ ekrana računala ili na druge načine.

Slika 3: Obavijest Otp banke. izvor: https://elementa.otpbanka.hr/otp-login/obavijest.html

Primjera internet prijevara ima još, to je područje koje se stalno širi te se stalno pojavljuju nove prijetnje i novi načini kako prevariti nepažljive internet korisnike. Krađom korisničkih

podataka od strane kriminalaca, korisnik riskira i veće posljedice od krađe novca. Krađom digitalnog indentiteta moguće je otvaranje naloga i ugovora, odnosno pravnih akata koji će korisniku prouzročiti i golemu materijalnu štetu, a moguće je i dovođenje u pitanje vlasništvo nad imovinom.

3.3. E-mail prijevare

Vrlo blisko povezane sa internet prijevarama i phishingom, jesu i e-mail prijevare. Zapravo se često radi o i povezanim načinima, jer phishing prijevare u velikoj većini slučajeva stižu putem e-mail usluge, a za njihovu provedbu se otvara pretraživač interneta i preusmjerava korisnika na lažnu stranicu, tako da se radi o procesu povezanih načina prijevara, no ima i manji broj onih koje se odvijaju putem e-maila. Iako ne sve, e-mail prijevare često s "druge strane" imaju pravu, živuću osobu, a ne skriptu[5]. Takvi, "lažni" e-mailovi se često šalju kompanijama, te se sadržaj e-maila barem djelomično prilagođava "meti". Znaju se slati e-mailovi koji zahtijevaju plaćanje za nepostojeće robe ili usluge, a kod "prometnih" kompanija gdje se broj takvih zahtjeva mjeri u stotinama ili više dnevno, moguća je nepažnja korisnika te automatsko, gotovo pa refleksno dodavanje vrijednosti iz lažnog računa u platne naloge. Ukoliko je račun ispisan na domaćem jeziku, i sa primateljem koji je u nekoj lokalnoj banci, vjerojatnost da će takav vid prijevare proći se još i povećava.

Slična situacija je i sa rezerviranjem smještaja, gdje se pošiljatelj e-maila predstavlja kao zainteresirani gost koji želi rezervirati smještaj, te je na prvi pogled takav e-mail legitiman i ne pobuđuje sumnju. Kroz komunikaciju sa "gostom" prijevara eskalira, te može imati nekoliko tipova zapleta. Prvi, najbrži, jest da "gost" pošalje poveznicu ili dokument u e-mailu, kojega će korisnik otvoriti te zaraziti računalo sa virusom koji je sadržan u dokumentu ili na poveznici. To su popularni cryptovirusi te će o njima biti riječi u idućem poglavlju[6]. Drugi tip jest da "gost" priloži valjani način plaćanja, a zapravo se radi o ukradenim kreditnim karticama. Ukoliko je korisnik, odnosno operater nepažljiv ili brzoplet, lako je moguće da će odraditi transakciju sa POS uređaja svog radnog mjesta i time oštetiti žrtvu krađe sa određenim iznosom. Nakon toga, gost šalje e-mail da se predomislio i da ne želi više rezervirati smještaj, te traži povrat novčanih sredstava na bankovni račun. Većina banaka dozvoljava da se u roku od 24-48 sati odradi povrat na kreditnu karticu, no

5 Izvor: Situacija koja se dogodila autoru
6 Izvor: Situacija koja se dogodila autoru

van tog vremena postaje potrbno povrat izvršiti virmanom na nečiji račun, te se tako prijevara dovršava. Ovakvi tipovi prijevara su česti u turističkim agencijama i recepcijama raznih turističkih objekata, gdje je količina sličnih e-mailova velika, i sadržaj sličan jedan drugome, te umoran ili nepažljiv operater može zbog čiste rutine napraviti kriminalno djelo.

Možda najstarija, najviše korištena te vjerojatno i najmanje uspješna metoda e-mail prijevare jest traženje pomoći direktnom novčanom uplatom. Često se pošiljatelj predstavlja rodbinom, prijateljem ili poznanikom te od korisnika traži novčanu uplatu kako bi se izvukao iz izmišljenog problema u kojega je upao. Iako je odmah očito da se radi o prijevari, i ovakvi tipovi prijevara imaju dozu uspjeha. Primjer e-maila kojeg je pisac dobio, na kojemu se vidi da se pošiljatelj nije niti potrudio ispraviti ime "pošiljatelja" da odgovara imenu na e-mail adresi.


Trebam tvoju pomoć

Davor Imenjak <polaris.hrvatska@gmail.com>
a

Oprosti što ti se javljam ovako. Otputovao sam u Kipar, i moja torba, u kojoj je bila putovnica i kreditne kartice su mi ukrali. Kontaktirao sam banku, ali treba im još vremena da mi naprave novu karticu. Mislio sam te zamoliti da mi posudiš nešto novaca koje cu ti vratiti po povratku. Treba mi 1.300 eura da pokrijem troškove. Mogu ti proslijediti detalje o tome kako vi možeš slati novac. Molim te javi mi je li to moguce. Željno iščekujem tvoj odgovor!

Dražen Rajković

...

Davor.

Slika 4: Traženje "pomoći" putem maila. Izvor: autor

U svima od navedenih prijevara moguće je da se od korisnika traže razni osobni podaci, brojevi kreditnih kartica, pa čak i pristupni podaci za određene servise poput društvenih mreža, e-mail usluge, prijave na internet bankarstvo i tako dalje. To bi sve bile krađe identiteta. Na ovakve prijevare može korisnik sam utjecati u većoj ili manjoj mjeri, ne ostavljajući svoju e-mail adresu na raznim portalima, stranicama, webshopovima, i slično. Iskusniji korisnici znaju da je odavanje vlastite e-mail adrese slično legitimaciji, prosječan građanin neće svakome odavati svoje ime i prezime ili broj mobitela, te bi se na isti način trebao ophoditi prema svojoj e-mail adresi. Na internetu postoji ogroman broj malicioznih portala, te "information dealera" koji prikupljenje e-mail

adrese preprodaju trećim osobama. Za potrebe "življenja" na internetu, pisac teksta strogo savjetuje otvaranje barem još jedne do dvije lažne e-mail adrese, koje nisu ničim povezane sa imenom i prezimenom korisnika, ili na drugi način povezane sa privatnim i poslovnim životom. Za sve riskantne, nepouzdane ili neprovjerene portale, stranice i webshopove, poželjno bi bilo koristiti lažnu e-mail adresu. Time bi korisnik ujedno bio siguran da ništa bitnoga neće dolaziti na tu e-mail adresu, a ostaviti će primarnu e-mail adresu čistom od nepoželjne pošte.

3.4. Spyware, malware i virusi

Radi se o malim programčićima koji se instaliraju ili pokreću zasebno, ponekad dolaze u kompletu sa legitimnim softverom, tj programima koje korisnik intencionalno želi instalirati na svoje računalo, dok češće ih instalira ili pokrene nepažnjom. Ponekad se preuzmu kroz internet pretraživač, klikom na reklamu ili animaciju na ekranu, ponekad se preuzmu zabunom, kada korisnik misli da preuzima legitimnu aplikaciju,a zapravo preuzima maliciozni softver. Često stižu i preko e-maila, maskirajući se kao pdf ili jpg dokument. Načina na koji oni mogu dospijeti na korisničko računalo evidentno ima više, no ono što im je zajedničko jest da se radi o samostalnim programima koji će dovesti u opasnost sam rad operativnog sustava, te predstavljaju prijetnju sigurnosti korisnika. Ovisno o tipu i njegovoj "intenciji", antivirusni softver ga može ali i ne mora detektirati, razlog više zbog kojega korisnik mora biti na oprezu. Određeni ovakvi nepoćudni programi će se instalirati, te samo korisniku izbacivati reklame dok normalno pretražuje internet, drugi će pratiti kretanje korisnika po internetu i snimati tipkovnicu, kako bi se domogao bitnih korisničkih podataka poput raznih online identiteta, kojima će preuzeti kontrolu nad njime i "izbaciti" korisnika. U moderno vrijeme, virtualni alter ego je korisnicima iznimno bitan, ako ne i bitniji od onog pravoga, s obzirom da nezanemarivu količinu vremena korisnici provode i "žive" na internetu, društvenim mrežama, IM servisima, e-mailu, i ostalim poslovnim portalima. Gubitak pristupa tako nekom servisu možda i ne bi bio toliko negativan, da se ne radi o preuzimanju, a ne o gubitku – korisnički identitet i dalje ostaje aktivan, ali on više nije njegov vlasnik, te ne kontrolira svoje radnje. Radi se o poprilično opasnoj situaciji,u kojoj treća osoba može preuzeti kontrolu nad nečijim poslovanjem, financijama, ali i gubitak pristupa društvenim mrežama ili e-mail servisu će prouzrokovati veliku količinu neugode i stresa.

Korak dalje idu virusi koji rade poveću štetu, vrlo često i štetu koju je nemoguće sanirati. Ovdje se misli prvenstveno na cryptoviruse, male programčiće koje antivirusi teško detektiraju jer

realno – i nisu virusi, već legitimni programi koji postoje za zaštitu korisničkih podataka, a zovu se cryptolockeri.

Slika 5: Primjer cryptolocker virusa. Izvor: https://sensorstechforum.com/wp-content/uploads/2017/04/remove-cryptolocker-2017-and-restore-encrypted-files-sensorstechforum-com.png

Takvi programi "zaključaju" korisničke podatke sa šifrom koju je nemoguće probiti, jedino kod cryptovirusa korisnik nije pod kontrolom o kojoj se šifri radi. U takvim slučajevima, cryptovirus će zaključati određene tipove dokumenata na korisničkom računalu, te će se i pokušati proširiti po mreži, kriptirajući i mrežne diskove. Najčešće zaključava poznate oblike dokumenata, slike, video zapise, glazbu, office dokumente, i slično, te na kraju korisniku javi da su mu dokumenti zaključani do daljnjega, te ponudi plaćanje otkupnine kako bi taj isti softver izvršio dekripciju podataka. Iznosi znaju biti pozamašni, reda veličine 500 eura/dolara na više. I dok će razne kompanije vjerojatno pristati na plaćanje ovakvog iznosa, pod uvjetom da su kriptirani bitni podaci, pojedinci često odustaju ili nisu u mogućnosti platiti takav iznos da vraćanje podataka. Ukoliko korisnik nije imao sigurnosnu kopiju na nekom offline mediju, ovo ujedno znači ostajanje bez podataka bez

mogućnosti za njihovim vraćanjem. Samo brisanje virusa s računala neće spasiti i podatke. Bilo koji tip nepoćudnih programa može uzrokovati i nematerijalnu, i materijalnu štetu, ovisno o tome kako je programiran, te se prepuštajući sigurnost samo antivirusnom softveru ne može biti sigurnim, stoga treba i paziti što se i kako se radi na računalu, te kojim programima se daju dozvole za pokretanje i instalaciju. Krađa korisničkih podataka je velik rizik kojemu se svakodnevno korisnici izlažu, samom činjenicom da koriste internet, te bi se trebali ponašati bolje prema vlastitim podacima. U vrijeme kada online identiteti predstavljaju korisnika na internetu, te ga prezentiraju drugima, kako u privatnom tako i u poslovnom životu, obzirnije ponašanje prema vlastitoj digitalnoj sigurnosti bi bilo itekako poželjno. Kao što većina ne bi nepoznatim osobama dijelila svoje dokumente i slike na cesti, ili im govorila svoje korisničke podatke za pristup raznim e-uslugama ili društvenim mrežama, tako ne bi trebala dovoditi te iste podatke u nesigurnost zbog nepromišljenog djelovanja na svom računalu.

5. VIRTUALNI IDENTITET

Svaki od korisničkih računa, koji će biti spomenuti dalje u radu, a počevši od e-mail adrese na dalje, predstavlja jedan identitet. To bi značilo da, na primjer, nečiji online identitet na društvenoj mreži, na forumu, na nekoj od mnogih MMO igara (engl. Massive Multiplayer Online) nije nužno isti, dapače, rijetko kada jest isti. Postoje osobe koje velik dio svojeg slobodnog vremena provode stvarajući svoj online identitet, gradeći virtualnu personu. To može biti određeni forum, gdje polako s vremenom pojedinac svojim sudjelovanjem u raspravama stekne određenu reputaciju, iako to varira ovisno o tematici foruma. Igrači online igara svoju reputaciju grade igranjem, te što su duže u igri i što su im statistike bolje, budu smatrani „profesionalnim igračima“. Upravo to napredovanje u virtualnom okruženju bude povod za prihvaćanje i poštovanje od strane drugih online korisnika. Pojedinac može toliko virtualnih identiteta imati, te biti toliko fokusiran na njih, da oni postanu važniji od stvarnog identiteta. Od kako postoje načini zarade upravo kroz napredovanje nečijeg online identiteta, stvarni identitet takvih osoba još više gubi na vrijednosti. Za primjer se može spomenuti igranje online igara, kada određeni igrač postane toliko dobar da stvori svoju publiku i fanove, uz određene online servise može dobivati donacije i određeni postotak od novčanog toka kojeg izazove. Jednostavnije rečeno – njegov online identitet počinje zarađivati realni novac. Takav način zarađivanja je dobio na popularnosti unatrag nekoliko godina, kada su otvorene platforme koje omogućuju interakciju gledatelja sa igračima. Za bolje shvaćanje principa rada, nužno ga je opisati. Naime, svaki korisnik koji se registrira na takvim platformama ima mogućnost objavljivanja video materijala. Ukoliko se radi o video materijalu koji ne podliježe autorskim pravima, korisniku je omogućeno financiranje, a točan iznos isplate se temelji na kombinaciji broja „sljedbenika“ tj. Broja korisnika koji prate njegov kanal i broja pregleda koje njegov video dobije. S obzirom da takve platforme u video ili preko videa objavljuju reklame, to je glavni vid zarade, a autoru videa ide određeni postotak. Na tom principu radi globalno poznat video servis Youtube. No postoje platforme koje su specijalizirane baš za igre , tj. g*ameplay.* Na takvim platformama igrači snimaju sebe tokom igranja na način da većinu slike čini sama igra, a u jednom njenom dijelu osoba koja ju igra, sa zvukom koji je najčešće kombinacija zvuka iz igre i govora igrača. Svaki igrač , tj korisnik koji objavljuje video materijal na takvim platformama ima mogućnost objave u stvarnom vremenu, što je zapravo i najčešći slučaj, a gledatelji imaju mogućnost ostavljanja komentara i slanja novčanih donacija autoru. „vlasnik“ kanala dobije postotak od iznosa kojeg njegov kanal ostvari putem reklama, ali i donacije korisnika. Takav vid online zarade je u novije vrijeme postigao ogroman uspjeh, ako je suditi po broju gledatelja, kao i po broju igrača koji na taj način zarađuju.

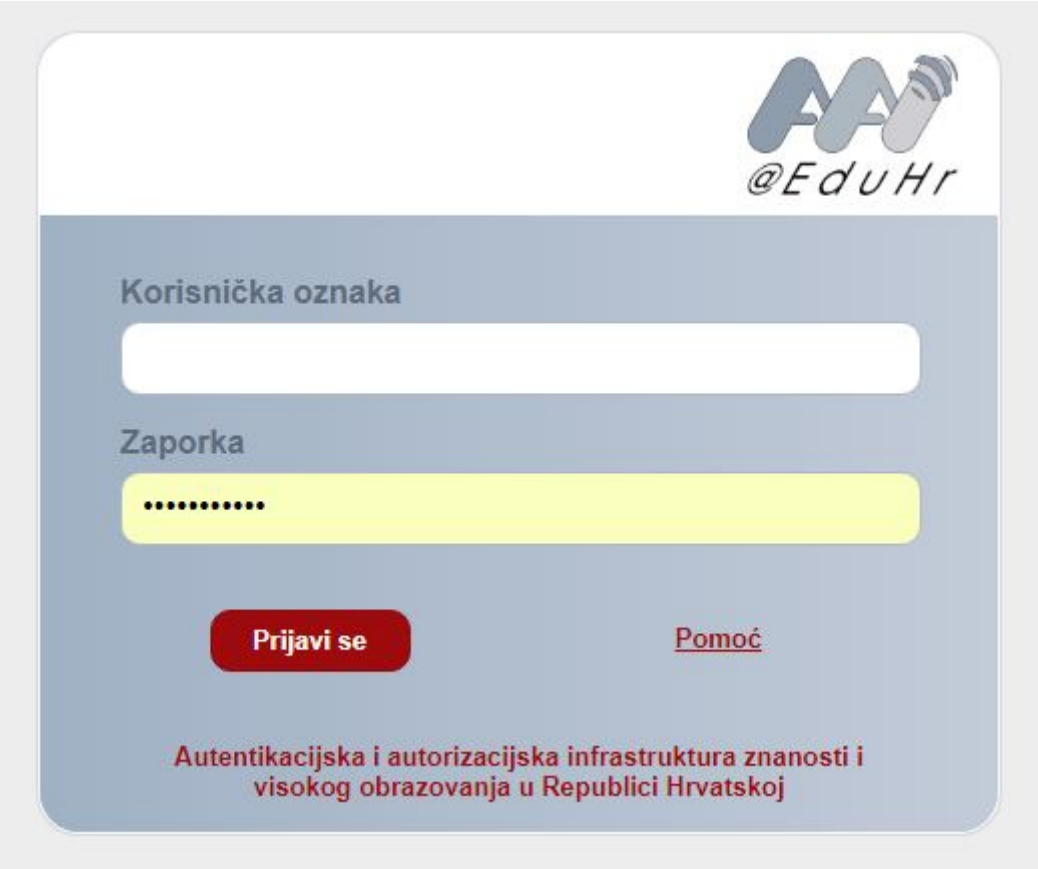
Jedna od karakteristika takvog „poslovanja“ jest da korisnik koji dobiva isplatu nije ni na koji način povezan s državom, ne postoje porezi, doprinosi i ostali državni nameti s obzirom da novčani tok ide mimo državnih institucija.

5.1 Digitalni identitet

Digitalni identitet predstavlja digitalnu formalnu reprezentaciju stvarne osobe, pod formalnim se misli na činjenicu da vlasnik-korisnik takvog identiteta nije ovlašen da taj identitet stvori ili mijenja, već to radi jedan od ovlaštenih državnih organa. Pod digitalnim identitetom se može smatrati e-osobna iskaznica, e-zdravstvena iskaznica, e-građani korisnički račun, e-vozačka dozvola, i tome slično, ukratko digitalni identitet koji neporecivo predstavlja fizičku osobu, kojom se ta osoba, pred zakonom, može identificirati. No digitalni identitet ne mora nužno biti i fizička isprava. Digitalne isprave omogućuju računalno očitavanje spremljenih podataka (unutar čipa na kartici, magnetnom zapisu ili RFID čipu) no podaci o korisniku su ionako centralno spremljeni na poslužiteljima odgovarajućih ministarstava, odnosno odgovarajućih institucija.

Još jedan od digitalnih identiteta koji je ujedno i prihvaćen na usluzi e-građani, jest CARNet-ov AAI@edu identitet, kojeg dodjeljuje CARNet učenicima, studentima i prosvjetnom osoblju, a koji osim korištenja usluga unutar RH, olakšava studentima identifikaciju i migraciju unutar ostalih članica EU, s obzirom da je AAI@edu račun međunorodno priznata mjerodavnica.

Da bi korisniku bio dodijeljen AAI@edu korisnički račun, korisnik mora CARNetu dostaviti svoje osobne podatke, uz potvrdu prosvjetne ustanove (škole, fakulteta) te mu naknadno bude dostavljen i aktiviran AAI@edu račun, kojim dokazuje svoj identitet kako na e-građani usluzi, tako i ostalim javnim tijelima koji prihvaćaju taj način autentifikacije.



Slika 6: Prozor za autentifikaciju studenta. Izvor: https://login.aaiedu.hr

Povezano sa AAI@edu računom, jest i JMBAG identitet. Radi se o jedinstvenom matičnom broju akademskog građanina, a koji potvrđuje svaku osobu koja ulazu u akademsku zajednicu, te stoji vezan za nju dok kraja života. Važno je napomenuti da se JMBAG razlikuje od JMBG-a, koji identificira svaku fizičku osobu u RH , dok JMBAG identificira svakog akademskog građanina. Promjenom visokog učilišta ili fakulteta, JMBAG se ne mijenja. Sastoji se od 10 znamenki, od čega prve 4 znamenke označuju visoko učilište (npr. 0066 označuje pravni fakultet u Zagrebu, 0069 označuje tehnički fakultet u Rijeci).

JMBG predstavlja jedinstveni matični broj građana, svakom građaninu RH prilikom rođenja bude dodijeljen njegov jedinstveni matični broj, mada je taj broj stečevina iz vremena Jugoslavije, s obzirom da se dodijeljuje od 1976. godine. Za razliku od OIB-a, iz JMBG-a se mogu iščitati informacije o korisniku, poput datuma rođenja, države i regije rođenja, te spola. Upravo iz tog razloga smatra se nesigurnim i podložan zloupotrebi, pa je u RH zamijenjen OIB-om, tj. Osobnim Identifikacijskim Brojem. Iako ni JMBG ni OIB nisu "digitalni" u smislu da ne zahtijevaju karticu ili čip za njihovo očitavanje, podaci o vlasnicima i sve osobne informacije su spremljene na

poslužiteljima odgovarajućih ministarstava RH, te svaka autorizirana javna institucija ima pristup i uvid u te podatke.

5.2. Virtualna zajednica

Društvenu virtualnu zajednicu se može opisati kao grupu ljudi koja se ne upoznaje ili sastaje u stvarnom svijetu, već komunicira putem interneta, poput društvenih mreža, foruma, blogova i ostalih mrežnih aplikacija. Cijeli svijet se pretvorio u globalno selo (eng. global village), posredstvom interneta moguće je pronaći događaje koji se u tom trenutku događaju tisućama kilometara daleko, moguće ih je vidjeti uživo, kao što je moguće pronaći događaje koji su se već dogodili, a podaci o njima su spremljeni negdje na internet poslužiteljima (eng. server) i moguće im je pristupiti i pregledavati ih. Društvene mreže idu korak dalje, nudeći često subjektivne, ali i objektivne, a ne „ušminkane“ verzije događaja poput onih koje serviraju TV kuće i senzacionalistički portali vođeni nečijom političkom rukom. Korisnici, oni koji se tog trenutka nađu u određenoj situaciji, da osobno prenesu vijesti, poput slike ili videozapisa, te da iste objave na nekoj društvenoj mreži, forumu ili posredstvom nekog drugog oblika digitalne komunikacije. Postoje nacije koje osim što prikrivaju društveno-političke događaje u svom dvorištu, vlastitim građanima zabranjuju pristup novostima iz svijeta ili regije, koristeći razne mehanizme cenzure o kojima će u naknadnim poglavljima biti riječi. Pomoću interneta, moguće je zaobići tu forsiranu cenzuru te pristupiti informacijama, pod uvjetom da informacije postoje. Ovdje se aludira na Sjevernu Koreju, ili Kubu, čiji politički režim, ali i ekonomska situacija spriječava ne samo dijeljenje podataka o događajima koji se u državi zbivaju, nego i priječi nastajanje zapisa od strane korisnika. Nepostojanje informatičko-komunikacijske infrastrukture, medija, i zapisa nije karakteristika samo Sjeverne Koreje mada je ona najbolji primjer, već i drugih zemalja trećeg svijeta, no bila je poanta naglasiti da, iako se svijet danas tretira kao globalno selo, u kojemu je moguće doći do podataka o svemu, to ipak nije slučaj. No postoji i jedna druga strana društvenih mreža i zajednica – umjesto da se pažnja pridaje velikim događajima koji zahvaćaju velik broj ljudi, upravo je mogućnost suprotnoga velika pozitivna strana. Pojedinci koji bi inače bili svijetu nevidljivi i čiji problemi teško da bi došli do očiju javnosti, putem društvenih mreža mogu pustiti svoj glas, ili vapaj za pomoći, u javnost. Mnogobrojne dobrotvorne akcije pokrenute su upravo na društvenim mrežama, od apela za pomoć oboljelih, onih kojima je izvršena velika nepravda, onih koji su uslijed neke više sile ostali bez svega, i tako redom, mogu pomoć tražiti na društvenim mrežama, gdje je velika vjerojatno da će se glas proširiti te će se pojedinci udružiti kako bi pomogli

unesrećenima. Takvih akcija ima često, a upravo su društvene mreže jedan od glavnih medija koji u takvim situacijama mogu pomoći. Moguće je da neka od tih priča završi u poznatim papirnatim medijima, poput dnevnih novina i njihovih e-izdanja, no mediji traže senzacionalističke vijesti, što bi privuklo čitatelje kako bi se prodao veći broj novina, ili kako bi e-izdanja i web stranice medija postigle veći broj pregleda. Nakon nekoliko objava, vijest prestane biti senzacionalistička, padne u zaborav te svoje mjesto prepusti drugim kratko živućim novostima. Društvene mreže imaju drugačiji koncept rada, a senzacionalizam i broj pregleda nije direktno povezan sa zaradom, s obzirom da korisnici društvenih mreža istu ne posjeduju, odnosno ne zarađuju njenim korištenjem. Također, popularnost društvenih mreža raste sve više i više, dostupne su svima, na svim digitalnim platformama, u bilo kojem trenutku. Ukoliko ih se usporedi sa tradicionalnim medijima, oni nemaju takvu pažnju publike, a ukoliko se radi o nekim lokalnim novinama, malo je vjerojatno da dođu u doticaj sa širom publikom, pa makar postojalo e-izdanje, i makar imali web stranice. Korištenje nesretnih situacija i događaja, poput ratova, zna biti korišteno u svrhu propagande, mediji cenzuriraju određene činjenice i iskrivljuju priču kako bi ona bila u nečijoj koristi, umjesto da objektivno prenose činjenice, na kraju stvorivši od tragičnih događaja samo vijest koju dio čitatelja neće niti pročitati do kraja, a kamoli se osjećati dužni pomoći na bilo koji način. Štoviše, često mediji indirektno potiču ljude da se okrenu jedni protiv drugih, prijeteći dodatnim negativnim posljedicama. Kod reportaža može i nedostajati onaj „drugi“ dio priče, poput pogleda na situaciju od strane onih koji su događaj doživjeli na vlastitoj koži. Malo koji medij će biti spreman prenijeti vijest koju im je dostavila fizička osoba. Društvene mreže nemaju taj režim rada, i iako je odluka hoće li se prenijeti neka priča, vijest, slika, događaj upravo na korisnicima društvenih mreža – bitno je da zapis postoji te ga je moguće podijeliti s javnošću.

5.3. Blogovi - mrežni dnevnici

Društvene mreže nisu jedini medij komunikacije koji ide u smjeru od korisnika prema javnosti. Mrežni dnevnici, poznati kao blogovi (eng. blog) su jedna od alternativa. Postoje okvirno od kraja devedesetih godina, nakon što su nastali web servisi koji su korisnicima omogućavali da objavljuju tekstove bez potrebe za znanjem html jezika. Skraćenica su od riječi *weblog*, a radi se o javnim objavama internet korisnika. Pretpostavlja se da postoji preko 315 milijuna blogova na internetu[7], no ta se brojka mijenja konstantno. Radi se o ogromnoj količini teksta kojeg internet korisnici pišu i objavljuju javno, no specifičnost bloga bi bila što ne zahtijeva publiku. Iako blogovi

7: https://infogr.am/number-of-blogs-worldwide

jesu javni, često su nebitni za ikoga osim za pisca, pa se blogove može shvatiti i kao javni dnevnik, knjigu misli, općenito sve što netko želi podijeliti sa svijetom, bez da traži povratnu informaciju o tome. Pisanje je ljudska potreba, a blog je savršena platforma za to. Naravno, postoje popularni blogovi, koji se tiču točno određene tematike, pisani od strane stručnih ljudi, ili samo onih koji su više upućeni u određenu temu. Kritike na političku, društvenu i ekonomsku situaciju su popularni tekstovi koji često imaju širu publiku, često vrlo subjektivnog tona, pisani od ljudi koji imaju ili samo misle da imaju nešto pametno za reći. Kako inače biva, takvi tekstovi stvore publiku istomišljenika te se blog, ili njegov autor, jedno vrijeme populariziraju upravo iz tog razloga, što izražavaju mišljenje određenog dijela stanovništva.

Kritike trenutnog društvenog uređenja nisu jedini popularni blog zapisi. Kao i kod društvenih mreža, tako je blog platforma koja omogućava da određena slabo praćena vijest ili događaj dospije do pažnje većeg broja ljudi. Za razliku od medija poput novina, koja ne mogu, ne žele ili im nije u interesu da prenesu neku vijest – profit je bitan za takve medije, a ne nosi svaka vijest mogućnost za profitom – na blogovima postoji sloboda govora, pa korisnici mogu prenijeti vijesti koje će veći mediji ignorirati. Primjer su razne eko-grupe i udruge za zaštitu životinja i prirode, čije objave veći komercijalni mediji malo kada prenesu.

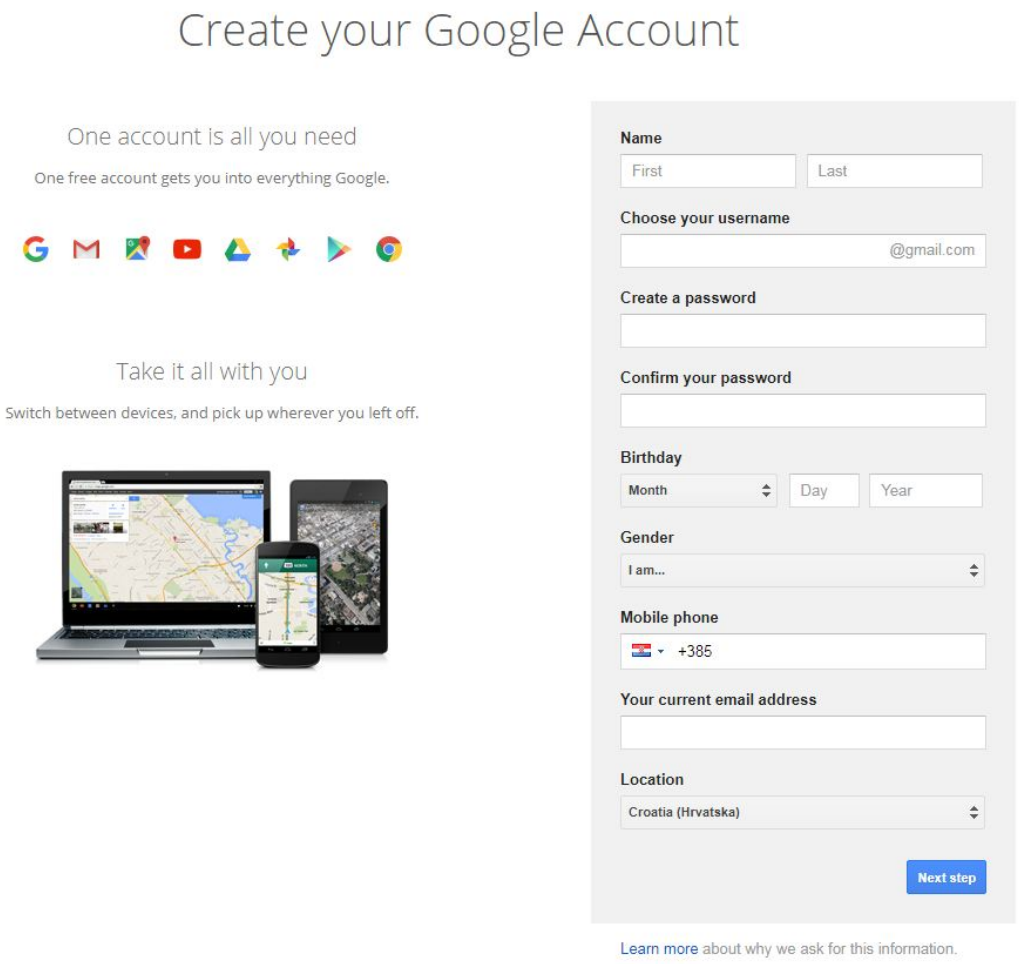
No blog platforma nije samo to. Korisnicima se omogućava objava slika i videozapisa, a podržavaju i komentare. Jedan od primjera osobnog bloga bi bio putopis. U moderno vrijeme digitalni aparati su standardna oprema na putovanjima, a kratki videozapisi su popularni za predočavanje događaja koji su se dogodili tokom putovanja. Objava putopisa je logična stvar za osobu koja voli putovanja, a ne želi se limitirati na društvene mreže (ili želi ostati anonimna). Dug i detaljan putopis, sa mnoštvom detalja potkrepljenih slikama i videozapisima čine jednu urednu cjelinu, te se putem objave na blogu javnosti pruži prilika da nakratko virtualno dožive tuđe putovanje. No i ukoliko nitko nikada ne pročita taj blog, osoba koja ga je napisala je ispunila svoju „obavezu“, odnosno sam čin pisanja potpomaže osjećaju ispunjenja obaveza. Računalo korisnika je ujedno i medij za pohranu osobnih podataka, no malo koji korisnik za svoje privatne potrebe radi tako temeljite i uokvirene tekstove poput onoga na blogu. Jedan od razloga jest što je kompliciranije i tehnički zahtjevnije: većina tekst editora ni danas ne podržava integriranje video zapisa, a jednom spremljen dokument postaje virtualno „težak“ jer su u njemu originalne slike i videozapisi, te kao takav nije jednostavan za dijeljenje. Ukoliko se koriste *hyperlinkovi* umjesto integracije zapisa, jednom kada se originalnom zapisu (slici, videu) promijeni lokacija na disku, čitav tekst gubi smisao jer prestaje biti cjelina, iz njega se povezani zapisi „izgube“. Stoga web objava čini logičan izbor za osobu koja želi neke svoje misli i događaje objaviti javno. Zadnjih nekoliko godina rastu na popularnosti vlogovi – video logovi. Umjesto tekstualnih objava na blogovima, korisnici snimaju

video logove, često kratke monologe sa isječcima iz ostalih video zapisa, stvarajući tako video alternativu blogovima. Takvi uratci se onda objavljuju na portalima koji nude korisnicima mogućnost *uploada* video zapisa. Naravno da je korisnicima dozvoljeno objaviti i video zapise ostalih sadrzaja (ukoliko nisu zaštićeni autorskim pravima ili se radi o pornografiji) pa korisnici, ukoliko se nalaze u blizini održavanja nekih manifestacija, objavljuju video isječke. Ukoliko se radi o aktivizmu, prosvjedima, ratu i slično, novinari znaju kasniti na lokaciju ili uopće ne otići, iz različitih razloga, pa su upravo korisnici ti koji „izvještavaju“ o stanju na terenu, a komercijalni mediji ili tv kuće tada preuzmu videomaterijal te ga, ako žele, objave.

5.4 E-pošta

Do sada je bilo riječi zapravo o platformama koje omogućavaju korisnicima objavu vlastitih vijesti, odnosno *postova* pod svojim imenom ili pseudonimom, kao i komentiranje na svoje i/ili tuđe objave. Da bi sama objava ili komentiranje bilo moguće, potrebna je „registracija“ korisnika čime on postaje korisnik određene mreže, foruma, odnosno zajednice. Kako bi to bilo moguće, pojedinac se mora registrirati, a uvjet za to jest davanje određenih osobnih podataka. Za razliku od digitalnog identiteta kojim krajnji korisnik često ne raspolaže otvoreno, a o kojemu će biti riječi naknadno, kod *online* identiteta korisnik ima apsolutno pravo nad upravljanjem svojim računom (engl. Account). Za njegovo kreiranje, gotovo pa obavezna stavka neovisno o platformi na koju se korisnik pokušava registrirati, jest *e-mail* adresa. Alternativa ponekad zna biti broj mobitela korisnika, na koji se pošalje aktivacijski kod za potvrdu identiteta. Dakle, da bi korisnik krenuo s korištenjem praktički bilo kakve platforme, mora potvrditi svoj identitet otvaranjem aktivacijskog koda kojeg platforma pošalje na danu e-mail adresu. Stoga, potrebno je prvo otvoriti e-mail račun. U RH i dalje vrijedi pravilo da svaki korisnik fiksne internet usluge od svog davaoca usluga (engl. ISP – Internet Service Provider) dobije i e-mail adresu, kao što svaki student hrvatskih fakulteta dobije e-mail adresu od CARNeta. Dakako korisnik nije obavezan istu koristiti, već može otvoriti e-mail račun anonimno preko bilo kojeg alternativnog davaoca e-mail usluga. Takvih ima poveći broj, koji se mjeri u tisućama pa i više, pa je moguće izabrati onoga za kojeg korisnik smatra da udovoljava potrebama. Prilikom registracije za e-mail adresu, potrebno je unijeti određene podatke, no nitko ne provjerava njihovu točnost, što znači da je moguće otvoriti račun bilo sa točnim osobnim podacima, bilo sa lažnima, kreirajući tako internet pseudonim kojim će se korisnik predstavljati internet populaciji. S obzirom da se internet smatra mjestom gdje vlada sloboda govora, no dokazalo se da to baš i nije u potpunosti točno te su određene osobe bile krivično gonjene zbog izražavanja svojeg mišljenja,

anonimnost pod krinkom pseudonima bi trebalo razmotriti prilikom kreiranja email adrese, te dakako kasnije prilikom davanja osobnih podataka raznim platformama.



Slika 7: Prozor kreiranja novog Google računa. Izvor: https://accounts.google.com/SignUp

5.6 Primjer kohezije digitalnog i online identiteta

Korištenje digitalnog i online identiteta naoko nisu povezani i nisu međusobno nužni kako bi se koristile razne online usluge, no česte su situacije kada je njihovo korištenje povezano i nužno, makar na prvu nije uočljivo.

Primjer kohezije jednog i drugog identiteta, gdje bez jednoga od njih se korisniku ne omogućuje korištenje neke (stvarne) usluge, bi bio turizam. Iako je turizam "offline" usluga i kao takva je i percipirana, ljudi koji odluče nekamo otputovati jednostavno otputuju na destinaciju i na lokaciji , jednom kada dođu, koriste sve turističke usluge koje žele. Tako se barem radilo do nedavno kad je internet preuzeo sve sfere turizma. Danas, od samog planiranja putovanja do njegove realizacije, koristi se internet bilo sa provjeru puta, narudžbu karata, bukiranje smještaja i ostale povezane usluge. Kombinacija tih usluga zahtijeva korištenje i online identiteta, i digitalnog. Naime, samim izlaskom iz matične države, vrši se provjera osobnih informacija zahvaljujući zapisu na osobnim iskaznicama, vizualni pregledi se koriste sve manje, a digitalna kontrola sve više i više. No i prije nego osoba fizički otputuje, vrlo često se odluči unaprijed rezervirati smještaj. Sve veći broj buking portala od korisnika zahtijeva da, osim kreiranja računa na samom portalu, time kreirajući online identitet za taj specifični portal, zahtijeva se i autentifikacija korisnika putem digitalnog identiteta. Za primjer se može spomenuti sve popularniji portal AirBNB, koji iako nudi gostima da se ne identificiraju[8] te nudi mogućnost rezerviranja smještaja gotovo pa anonimno, sve veći broj pružatelja smještaja zahtijeva da se njihovi gosti identificiraju njihovim osobnim dokumentima. Prilikom registracije na portal, korisnika se traži da unese 2 tipa dokumenata, prvi se odnosi na financijski dokument, tj. na kreditnu karticu, kako bi se rezervacija smještaja mogla naplatiti. Drugi dokument je osobna iskaznica, od korisnika se traži sken dokumenta ili upis broja dokumenta (broj osobne iskaznice, broj putovnice) koje se provjerava te nakon provjere se korisniku dopušta da rezervira i one smještajne jedinice za koje vlasnik traži identifikaciju gosta. Iako ovakvih primjera ima još, turizam je sfera gdje ima puno pogrešaka i prevara. Ovim načinom, pokušava se njihov broj svesti na minimum, s obzirom da iako su krađe dokumenata moguće, kombinacija krađe 3 vrste identiteta se ipak mjere u drastično manjem postotku, samim time osiguravajući da će korištenje turističkih usluga biti manje opasno. Sličnu stvar provode sve aviokompanije, gdje se korisnik provjerava pri ulasku na aerodrom, pri ulasku na avion, te pri izlasku sa aviona a prije ulaska u zemlju na destinaciji, no kontrola se vrši samo digitalnim identitetom, i to putnog dokumenta, dok se kupnja aviokarte može odvijati "analogno", plaćanjem u

8 Izvor: osobno iskustvo autora teksta

gotovini i bez kreiranja nikakvog online identiteta. Mada je stupanj sigunosti na zračnim lukama iznimno visok, ipak se radi o dva odvojena primjera čija je povezanost leži u činjenici da se, za dolazak na destinaciju, često putuje avionom. Stoga, zapravo je rezervacija smještajnog objekta ona koja bi se mogla opisati kao najtemeljitije provjerenom, s obzirom da korisnik mora proći nekoliko provjera.

6. ONLINE IDENTITET

Online identitet spada u digitalni identitet, kako je već ranije objašnjeno. Online identiteta koje korisnik može napraviti postoji velik broj, počev od onog najpopularnijeg – email računa. Doduše već godinama je možda email račun pao u popularnosti, s obzirom da svoje korisničke račune na društvenim mrežama otvaraju osobe koje nemaju nužno i email. Po procjenama, najveća društvena mreža- Facebook, ima milijardu i 790 milijuna aktivnih korisnika, dok tri najveća email servisa – gmail i yahoo mail imaju po milijardu, dok Microsoftov Outlook ima 400 milijuna korisnika. Ostalih email providera ima poveći broj, možda vrijedan spominjanja i njemački GMX mail koji broji oko 11 milijuna korisnika, no svi ostali, po broju korisnika, su zanemarivi u odnosu na tri velikana spomenuta ranije. Email je na prvom mjestu, kad je riječ o online identitetu, zato što je najbitniji za kreiranje virtualne osobe. Kako bi se korisnik interneta mogao "kretati" po Internetu i aktivno ga koristiti, nužno mu je potrebna email adresa. Alternativno može poslužiti i telefonski broj, no samo za manju količinu sadržaja. Osim toga, telefonski broj spada u "privatne" informacije, nikako nešto što će korisnici olako ostavljati po stranim portalima. Dakle, sve kreće od email računa. Za potrebe ovog rada, pretpostavit će se korištenje jednog od tri ranije navedena email servisaa, Gmail, Yahoo mail, ili Outlook. S obzirom da je email "polazna točka", za otvaranje su potrebni samo osobni podaci, koji ne moraju nužno biti povezani sa realnom fizičkom osobom. Bitno je samo ostvariti pristup email servisu. Korisnik prilikom registracije, "otvaranja računa" bira sigurnosnu šifru, kojom će zaštiti svoj račun, te se nakon toga uspješno po prvi put spojiti na svoj pretinac e-pošte.

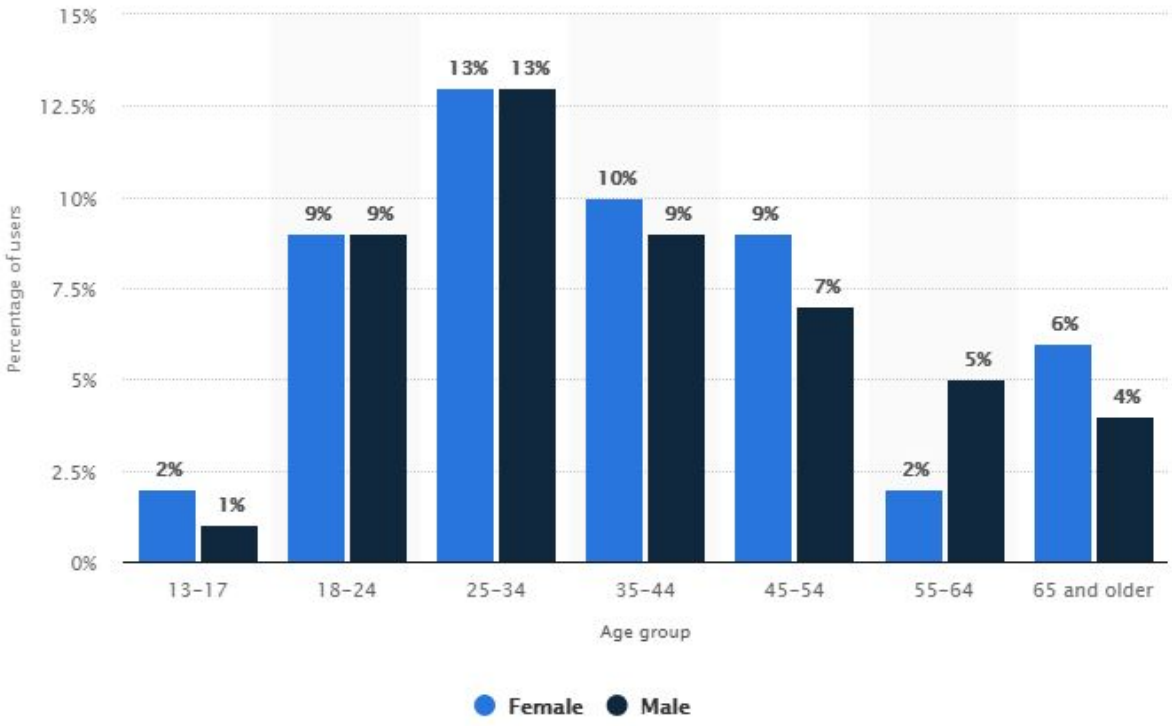
Koji će servis korisnik izabrati je savršeno individualan izbor. Jednom kreiran email račun, korisnik može nastaviti s korištenjem interneta u sve ostale svrhe. Kreiranje email računa je bilo bitno iz razloga što velik broj portala, stranica, servisa , društvenih mreža i slično od korisnika traži registraciju uz korištenje email adrese, koja se koristi za potvrdu identiteta. U današnje vrijeme, gotovo je nezamislivo aktivno korištenje interneta bez email adrese. Štoviše, korisnicima se

olakšava registracija i korištenje velikog broja portala jednostavnom prijavom kroz, npr, Gmail, gdje portal dobija informaciju o identitetu korisnika kroz sam email "profil". Naime, korištenje Google email servisa, automatski uključuje i kreiranje korisničkog identiteta, koji je uz autorizaciju vidljiv svim povezanim portalima. Ukoliko portal A traži registraciju korisnika, ali postoji i opcija "prijave" putem Gmaila, portal dobija pristup korisničkim podacima direktno kroz online identitet korisnika. Takav vid korištenja portala je sve češći, s obzirom da samo jednim klikom omogućava registraciju korisnika, koji ne moraju unositi sve svoje privatne podatke, već se oni samo "provjere" kroz google račun.

Nakon email-a, vjerojatnost da se korisnik želi registrirati na neku od društvenih mreža je poprilično velika. Najveća društvena mreža – Facebook, broji gotovo dvije milijarde aktivnih korisnika. Gmail i Yahoo mail servisi zajedno imaju upravo dvije milijarde korisnika, no nije dostupan podatak o tome koliko je tih korisnika zapravo "aktivno" odnosno koji broj aktivno koristi e-mail uslugu, pa direktna usporedbna nije moguća. Uzevši u obzir želju za otvaranjem računa, odnosno profila, na Facebooku, od korisnika se traži određeni minimum osobnih podataka, poput imena, prezimena i datuma rođenja. Kao i u slučaju e-maila, podaci ne moraju predstavljati realnu osobu, već je poanta su stvaranju digitalnog identiteta, virtualne osobe, kojom će se korisnik predstavljati na internetu. Iako za normalno pretraživanje i "surfanje" po Internetu nije nužan nikakav online identitet, osobito ako korisnik nema aspiracija da ostavlja svoj trag (u vidu komentara, postova, objave slika, i slično), postojanje i korištenje online identiteta omogućuje mu podešavanje određenih opcija i olakšava i poboljšava iskustvo pretraživanja interneta i korištenja raznih online servisa. Kreirajući profil na društvenim mrežama, naročito na Facebooku, olakšava mu pristup i komentiranje *news* portala, tj. Portala na kojima se objavljuju novosti i vijesti, portala sa određenom tematikom, jednostavno korištenje foruma koji omogućavaju korištenje Facebook profila za registraciju, i tome slično. Korištenje google računa omogućava korisniku da podesi specifičnosti pretrage i pohrani postavke, poput jezika, matične zemlje, načina prikazivanja rezultata i ostalih opcija.

Glede otvaranja korisničkih računa, kako na Google-u, tako da Facebooku, postoji klauzula o starosti, prema kojoj djeca mlađa od 13 godina nesmiju posjedovati račun, odnosno imati online identitet. No, trenutno niti jedan servis ne provjerava realnu dob, već samo prihvaća uneseni datum rođenja kao jedinu provjeru. To znači da, iako statistički nema korisnika ispod 13 godina starosti, a ankete niti ne prikazuju broj korisnika od 13 do 18 godina, takvi korisnici postoje, što je i realno za očekivati, s obzirom da se u većini škola informatika uči od prvog razreda, te su djeca od 7 ili 8 godina starosti više nego sposobna koristiti Internet i društvene mreže. Štoviše, djeca u sve ranijoj

dobi postaju vlasnicima pametnih telefona, gotovo pa automatski s time postajući korisnici društvenih mreža.



Slika 8: Demografski prikaz korisnika Facebook mreže. Izvor: https://www.statista.com/statistics/187041/us-user-age-distribution-on-facebook/

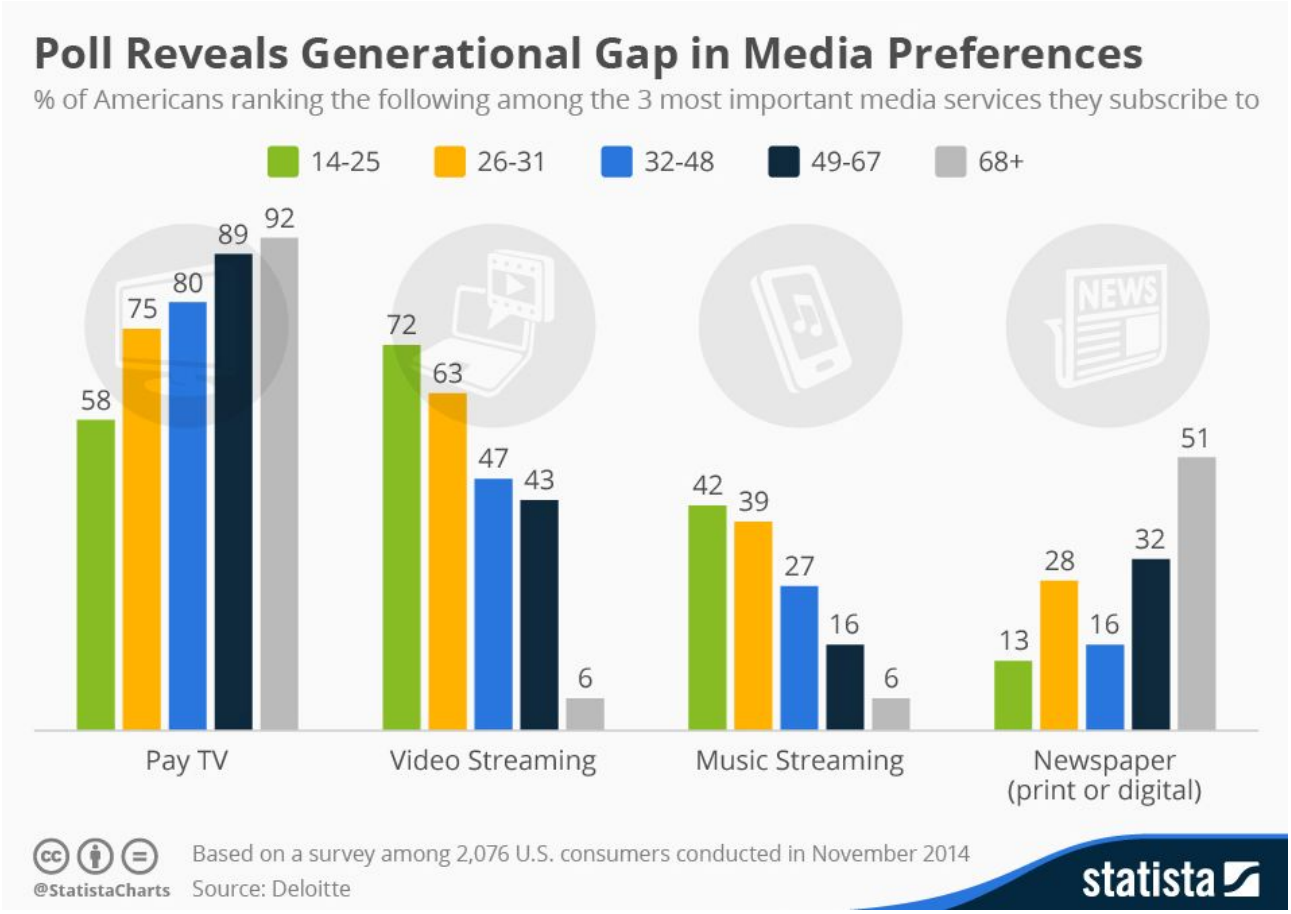
Online identiteta naravno ima poveći broj, i bilo bi nemoguće ih sve nabrojati. Ovisno o tome čime se korisnik bavi, postoje usluge koje tu oblast pokrivaju. Jedna vrlo popularna platforma koja kombinira fotografiju i društvene mreže je Instagram, na kojoj korisnici objavljuju svoje fotografije i omogućuju ostalim korisnicima da ih prate, komentiraju i favoritiziraju fotografije. Platforma je nekoliko godina unatrag, nakon što ju je Facebook kupio, doživjela pravi *boom* i postala *de facto* servis za razmjenu fotografija i iskazivanje vlastitih fotografskih (i umjetničkih) sposobnosti.

Iako ju se može smatrati glavnom platformom za dijeljenje fotografija, obzirom na popularnost i broj korisnika, platformi koje su strogo orijentirane na fotografiju i umjetnost ima još, a njima gravitiraju "pravi" fotografi i "pravi" umjetnici, kojima je cilj da na temelju svog rada i zarade. Ovdje se misli na Flickr i DeviantArt, dva velika servisa za objavu radova uz mogućnost komuniciranja sa ostalim korisnicima. Profesionalni fotografi često svoje radove objavljuju na Flickr-u, objavljujući fotografije u visokoj rezoluciji, kao što i umjetnici (crtači, animatori, ali i fotografi) koriste DeviantArt za vlastitu promidžbu i unapređivanje svojih sposobnosti. Osjećaj

pripadnosti zajednici je na takvim portalima drastično veći, jer se radi o platformama koje na neki način "prisvajaju" osobe sa istim ciljevima i istim interesima, za razliku od Instagrama koji je više "populistička" platforma gdje korisnici ležerno samo pregledavaju fotografije, bez da se previše upoznaju sa autorom.

Još jedan iznimno bitan društveni portal, koji je ujedno i najpopularniji video servis na svijetu, jest Youtube. Iako je započeo kao platforma za dijeljenje video uradaka, danas je puno ozbiljniji, sa velikim brojem kvalitetnih korisnika, koji kreiraju svoj video sadržaj upravo za korisnike te platforme. Za razliku od prije navedenih portala na kojima se korisnici "reklamiraju" i nude svoje usluge trećim stranama, kreiranje sadržaja i njihova objava na Youtube-u je samo sebi cilj, obzirom da Youtube svojim korisnicima isplaćuje naknadu, time se pretvarajući u pravog poslodavca. Iako portal omogućava objave bilo kakvih videa, u skladu sa svojim ugovorom o korištenju, sve je popularnije kreiranje sadržaja čiji su krajnji korisnici također korisnici platforme. Na temelju broja "pretplanika" na kanalu korisnika koji objavljuje video uratke, kao i ukupnom broju pregleda svakog videa, korisniku se isplaćuje određena naknada kojom se korisnika "nutka" da nastavi sa novim objavama, često rezultirajući osobnim napretkom i povećanjem kvalitete sadržaja. Upravo zahvaljujući toj poslovnoj politici, kao i popularnosti samog formata koji korisnicia-stvarateljima nudi novčane nagrade, a korisnicima-gledateljima nudi da si sami biraju što ih zanima i koga će gledati, na temelju istraživanja iz 2015. godine, Youtube je preuzeo ulogu "glavne video platforme" za korisnike dobne skupine 13-24 godine, time prestigavši i plaćene platforme poput Netflixa, kao i klasičnu televiziju koja emitira "zastarjeli" i "nebitan" video sadržaj.[9]

9 http://variety.com/2016/digital/news/millennial-gen-z-youtube-netflix-video-social-tv-study-1201740829/



Slika 9: Statistika popularnosti medija ovisno o starosnoj dobi korisnika. Izvor: https://d28wbuch0jlv7v.cloudfront.net/images/infografik/normal/chartoftheday_3457_poll_reveals_generational_gap_in_media_preferences_n.jpg

Ovo istraživanje se odnosi samo na koristike u SAD-u, na kojima se istraživanje baziralo, ali realno je pomisliti da isto stanje vlada i u drugim državama.

6.1. Dijeljeni resursi

Nakon navedenih najpopularnijih i najopćenitijih oblika online identiteta, koje gotovo svaki Internet korisnik posjeduje, postoji još velik broj ostalih, no oni su opet individualni, u smislu da ih korisnik koristi za svoje potrebe, onda kada to želi i kako to želi. No postoji i jedan drugi oblik online identiteta, kod kojega korisnik postaje svrha drugim korisnicima. Bolje rečeno, njegovi računalni resursi su dani na upotrebu drugim korisnicima. Ovdje će biti riječi o nekoliko tipova društveno dijeljenih računalnih resursa.

6.2. Dijeljenje podataka

Još od samog početka Interneta, isti je bio korišten za dijeljenje podataka, koje se u ono vrijeme najviše baziralo da serverima administriranima od strane raznih poslovnih subjekata, ponajviše zbog cijene samih servera, ali i zbog potrebe za posjedovanjem velikog broja modemskih ulaza putem koji su se korisnici spajali na servere. Od početka 90ih godina, brzine pristupa su se povećavale s odmakom vremena i napretkom tehnologije, počevši od prvih iskoristivih brzina od 14.4kbit, do maksimalnih 56kbit koliko su telefonske linije, odnosno analogni modemi podržavali. Iako tehnički moguće, dijeljenje podataka među korisnicima nije bilo popularno radi niske brzine prijenosa, uzevši u obzir da je za vrijeme trajanja konekcije telefonska linija bila zauzeta, kao i cijene samog pristupa. Tek razvojem tehnologije koje je omogućilo povećanje brzina prelaskom sa analognih modema na novu "digitalnu" tehnologiju, odnosno na širokopojasni pristup, dijeljenje podataka između korisnika je postalo popularnije. Razvijene su čitave mreže i novi protokoli koji su međusobno spajali korisnike, omogućavajući da na jednostavan način dođu do traženih podataka. Za razliku od prethodnog načina, gdje su se podaci čuvali na serverima, razvoj aplikacija, mreža i protokola za dijeljenje podataka je promijenilo način rada – podaci su se nalazili na računalima samih korisnika, te su se preko specifičnih mreža, korisnici međusobno povezivali i dijelili podatke.

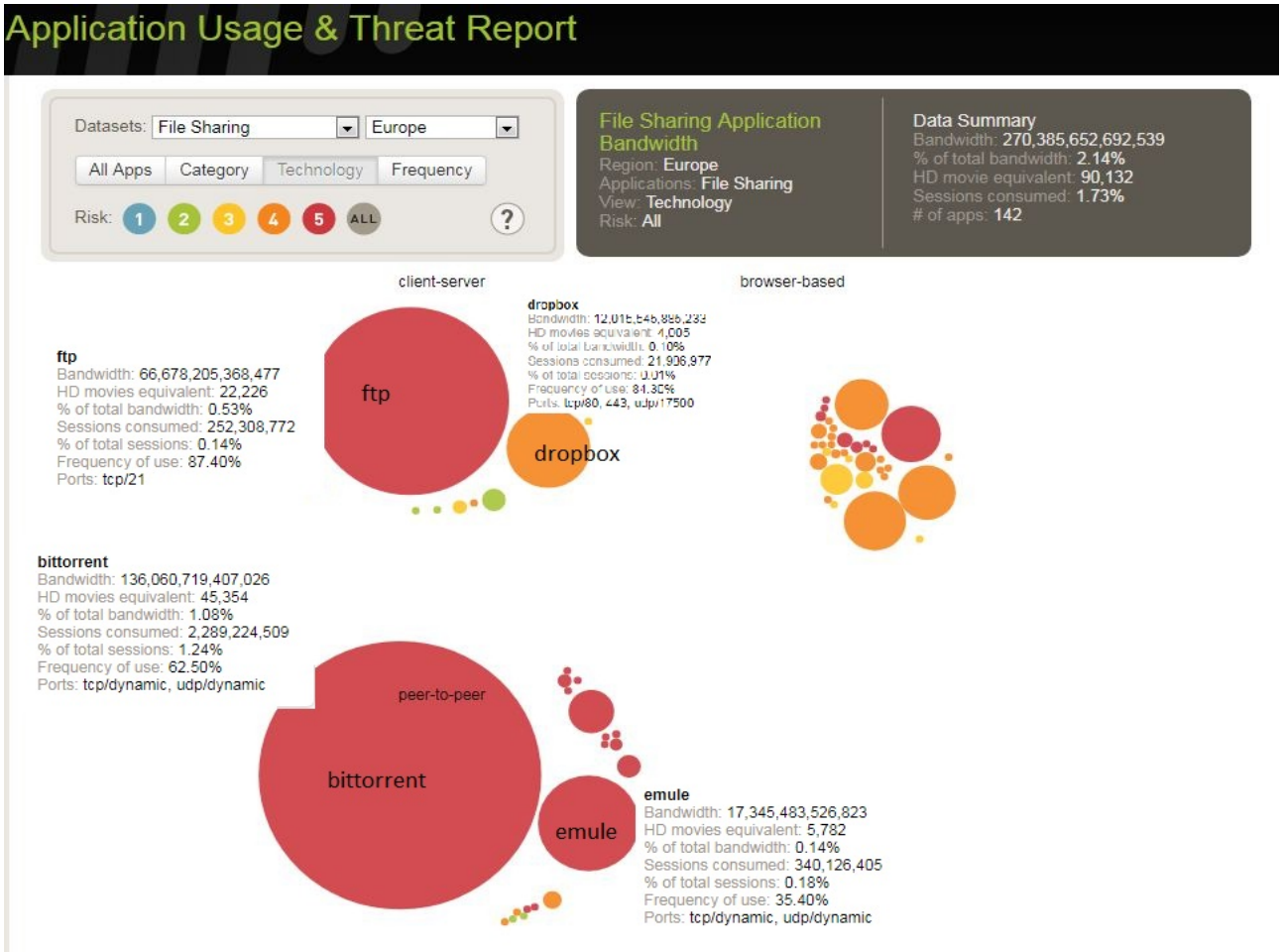
Zadnjih godina korisničko dijeljenje podataka, tj. p2p promet (engl. peer to peer) raste sve više, podaci iz 2017. nisu dostupni, no prema istraživanjima iz 2010. godine, u Europi je 10% ukupnog Internet prometa otpadalo na p2p promet, a po podacima iz 2004. godine, promet putem ovog protokola je činio 25% ukupnog Internet prometa na svjetskoj razini.[10] Realno je za očekivati da se zadnjih godina taj postotak povećao. Po podacima iz 2013. godine, prijenos podataka putem ovog protokola je zauzimao 3.35% ukupnog svjetskog mrežnog kapaciteta. [11]

Iako, s korisničke strane gledano, online identitet nije potreban za razmjenu podataka, gledano sa strane samog p2p protokola, svaki korisnik spojen na mrežu, automatski svako računalo spojeno na mrežu, ima svoj online identitet, u vidu ID-a, tako da protokol prepoznaje tko je zatražio koji *file* i kamo ga mora poslati. Gotovo pa neprimjetno, korištenjem p2p mreža korisnici čine određenu vrstu društvene zajednice, iako nisu u očitom kontaktu, oni svi sudjeluju u razmjeni podataka te spadaju u korisnike p2p mreže. Štoviše, iako za korištenje p2p mreža nije nužna komunikacija s ostalim korisnicima , ovdje ne misleći na mrežnu komunikaciju radi razmjene već tekstualnu komunikaciju između samih korisnika, oni često ipak sudjeluju u barem jednom vidu

10 https://torrentfreak.com/bittorrent-still-dominates-global-internet-traffic-101026/
11 http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization/

društvene komunikacije, a to su forumi , gdje se razmjenjuju podaci uz mogućnost razgovora, komentiranje i aktivno sudjelovanje u administriranju i postavljanju novih podataka. O samim forumima će biti riječi naknadno. Drugi manje društven, iako još uvijek vid komunikacije jest ostavljanje komentara na portalima koji se bave dijeljenjem podataka , takozvani *trackeri*, poslužitelji čija je svrha čuvanje indeks podataka i omogućavanje da korisnici dolaze do istih. Ovo najviše vrijedi za *bittorrent* protokol, s obzirom da on zahtijeva inicijalno preuzimanje indeks datoteke da bi počela razmjena podataka.

Iako je ideja p2p mreža da se podaci anonimno dijele te p2p mreže nisu zamjena za tradicionalno dijeljenje podataka putem poslužitelja, radi niske cijene, praktički besplatno, velik broj društveno orijentiranih projekata, odnosno projekata otvorenog koda (engl. open source) , poput raznih Linux distribucija, nudi opciju preuzimanja instalacijskih datoteka putem p2p mreža, čime se smanjuje zauzeće vlasitih servera i smanjuje upotreba resursa vlastite mreže. Kod manjih distribucija, koje nemaju vlastiti server, ovo drastično olakštava razmjenu i preuzimanje instalacijskih datoteka.



Slika 10: Prikaz korištenja bandwidth-a po protokolima. Prikaz pokriva samo Europu. Izvor: http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization/

Čak i veće kompanije, poput Blizzarda, koja proizvodi video igre (npr Diablo i World of Warcraft, čija se baza korisnika mjeri u milijunima, prema podacima iz 2014. godine, samo World of Warcraft je imao 100 milijuna igrača[12]. Blizzard koristi *bittorrent* protokol za ažuriranje igara i slanja dodataka, s obzirom na broj korisnika, ovo drastično ubrzava preuzimanje takvih datoteka, osobito iz razloga što, kada velik broj korisnika krene istodobno preuzimati podatke s istog servera, pad brzine je očekivan. Korištenjem p2p mreže, korisnici preuzimaju podatke od ostalih korisnika, a s obzirom da bittorrent protokol sadrži određene "pametne" algoritme prepoznavanja lokacije korisnika i rutiranja podataka na mreži, može prepoznati koji korisnici su međusobno "blizu", tj da se nalaze u istoj državi, te time ubrzati razmjenu podataka upravo između tih "bližih" korisnika, a ujedno manje opterećujući međunarodne linkove Internet providera. Postoje i ostale, manje popularne ili sad već neaktivne p2p mreže, kod kojih je mogućnost komunikacije između korisnika od početka bila dostupna, poput *edonkey* mreže , koja je velikim dijelom napuštena, ali i dalje drži okupljenu zajednicu korisnika koji iz određenih razloga ne žele ili ne smiju koristiti ostale otvorenije p2p mreže. Kod *edonkey* mreže, tj klijenata koji koriste tu mrežu, razmjena podataka ide direktno bez posredstva poslužitelja, prilikom pretrage vrši se pretraživanje svih spojenih korisnika u tom dijelu mreže, te se prilikom nalaska ciljanog file-a, korisnik "klijent" spaja direktno na korisnika "poslužitelja" i kreće s preuzimanjem traženog podatka, te se tada otvara direktna veza između ta dva korisnika, omogućujući i direktnu tekstualnu komunikaciju. Ovakav vid komunikacije nije popularan, a ni praktičan, no zna biti koristan. Iako je broj korisnika u konstantnom padu još od 2007. godine , ovo je još uvijek druga najpopularnija p2p mreža, nakon *bittorrent-a* . [13]

Općenito govoreći, upotreba p2p mreža spaja korisnike u društvenu mrežu na jedan ne toliko vidljiv način, barem s korisničke strane, no gledano sa strane servera, svako računalo-korisnik p2p mreža pripada toj p2p mreži, pa automatski i svaki korisnik računala koje je spojeno na p2p mrežu, pripada društvenoj zajednici.

6.3. Društveno dijeljeni resursi

Već od davnih dana , odnosno početaka korištenja računala za razne izračune, velike korporacije i vlade su gradile i koristile superračunala, koji su imali moć procesiranja daleko veću

12 http://www.polygon.com/2014/1/28/5354856/world-of-warcraft-100m-accounts-lifetime
13 http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2007.pdf

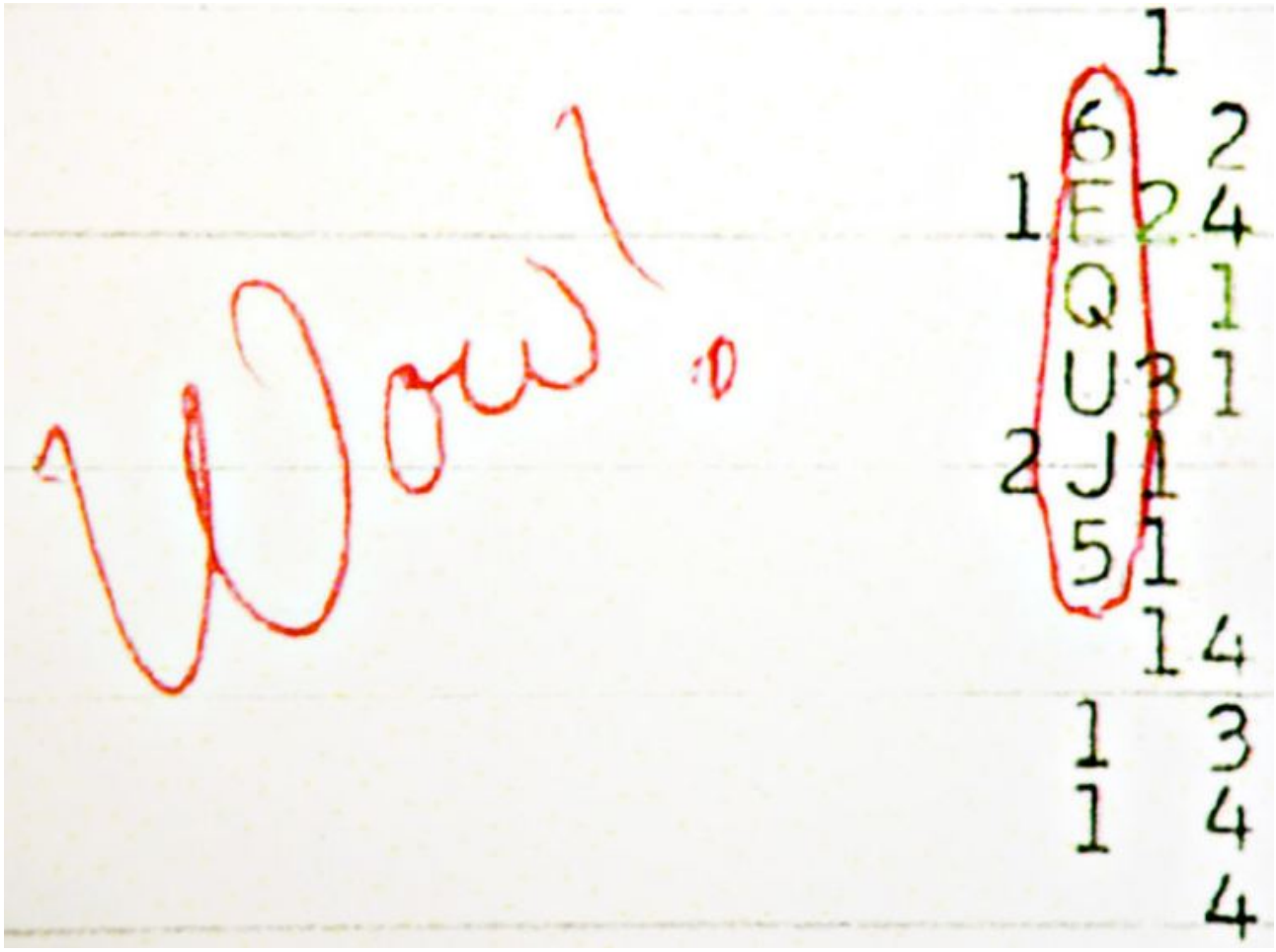
od "običnih" računala kakve su imali normalni korisnici, tj. onu koju su imala "osobna računala". Počela su se koristiti tokom 60ih godina prošlog stoljeća (*Hardware software co-design of a multimedia SOC platform* by Sao-Jie Chen, Guang-Huei Lin, Pao-Ann Hsiung, Yu-Hen Hu 2009, str 70–72), te su do 70ih godina sadržavala desetak procesora za paralelni rad. Kako je vrijeme prolazilo, tako se broj procesora povećavao, pa su tako do 90ih godina superračunala ima po nekoliko desetaka tisuća procesora. Ne ulazeći sada u detalje rada superračunala, bitno je napomenuti samo da je njihov rad , kao i sama konstrukcija, iznimno skup. Osim što treba sastaviti računala koja će imati tako velik broj procesora, sa adekvatnim hardverom, treba uzeti u obzir i veličinu takvih superračunala, kao i toplinsku disipaciju, zbog koje treba dizajnirati i napraviti adekvatan prostor gdje će se računalo nalazili, a koje mora imati i dobro izveden sustav napajanja. Kod velikih korporacija kao i vlada, koje imaju veliku financijsku moć, nije čudno vidjeti superračunalo. Korporacije, osobito medicinske, mogu veliku procesorsku moć takvih superračunala koristiti za analize DNK i ostale analize, vlade mogu koristiti takva računala za svoje privatne potrebe ili za razvoj, npr NASA ima svoje vlastito superračunalo koje broji preko 200 tisuća procesora i koje se koristi za modeliranje svemirskih misija. [14]

Ostale tvrtke koje imaju potrebu za kompleksnim izračunima, a koje nemaju financijsku moć da nabave superračunalo, često iznajmljuju procesorsko vrijeme komercijalno dostupnih superračunala, u prijevodu, kompanije koje imaju superračunalo, prodaju njegovo procesorsko vrijeme. Moguće je iznajmiti superračunalo, ali ne fizički, već se njegovi resursi dodijeljuju kupcima za određene izračune, te tako zainteresirani kupac može "iznajmiti" procesorsko vrijeme koje je potrebno za neki svoj projekt ili analizu.

No kod određenih projekata koji nemaju kraj, odnosno projekti traju "do daljnjega", takvo iznajmljivanje je preskupo, kao i gradnja superračunala. Za ovakve potrebe su razvijeni sustavi za dijeljenje izračuna, odnosno za društveno-dijeljene resurse. Ovdje se to odnosi na umrežavanje udaljenih, individualnih računala, kako bi se određeni izračuni odvijali na njima, dok bi se samo rezultati slali natrag na centralni server. Takav oblik dijeljenja resursa udaljenih računala zove se "distribuirano računanje" (engl. distributed computing)[15]. U biti radi se upravo o tome da se velik broj računala umrežuje kako bi se moglo iskoristiti njihove resursa radi paralelizacije procesiranja. Takva upotreba računala postoji još 80ih godina, mada točan početak nije zabilježen jer se radilo o manjim i privatnim projektima, 1985. održana je europska konferencija o distribuiranom računarstvu.[16] Sam princip rada i masovnu upotrebu popularizirao je jedan društveno-koristan

14 https://www.nas.nasa.gov/hecc/resources/pleiades.html
15 Benkler, Yochai (2006). “The Wealth of Networks: How Social Production Transforms Markets and Freedom”
16 http://www.disc-conference.org/

projekt, poznat pod nazivom SETI@home (čita se: seti at home) , iako nije prvi, to je možda najpopularniji projekt, koji na računala svih spojenih računala šalje podatke koje prikuplja Arecibo radio teleskop[17], a sa svrhom analize prikupljenih radio signala, ne bi li se dokazalo postojanje izvanzemaljskog života. Teleskop konstantno prikuplja podatke iz svemira, jedan dan prikupljenih podataka zauzima okvirno 1TB podataka, koji se za potrebe projekta SETI@home dijeli na velik broj dijelova, koji se šalju korisnicima na analizu. Sam projekt SETI (akronim od "Search for ExtraTerrestrial Intelligence) postoji još od kraja 19. stoljeća, a popularizirao se 1977. godine kada je otkriven jak signal iz svemira, takozvani WOW! signal[18].



Slika 11: Jak signal iz svemira, nepoznatog izvora, zbog jačine nazvan "wow" signal. Izvor: https://www.npr.org/sections/krulwich/2010/05/28/126510251/aliens-found-in-ohio-the-wow-signal

Projekt SETI@home je pokrenut 1999. godine, te je do sada imao preko 5 milijuna korisnika koji su za potrebe projekta "iznajmili" svoja računala, kako bi isti analizirali signale iz svemira.

17 http://www.naic.edu/

18 http://www.npr.org/sections/krulwich/2010/05/28/126510251/aliens-found-in-ohio-the-wow-signal

Projekt dan danas postoji i aktivan je, u ponešto izmjenjenom izdanju, odnosno unaprijeđenom kako bi podržavao nove računalne platforme.

Osim ovoga, ima još velik broj primjera projekata koji koriste distribuirano računarstvo za obavljanje izračuna, također u astroanalitičkoj sferi, ali i ostalima. Zadnjih godina se popularizirало korištenje distribuiranog računarstva u kriptografske svrhe, odnosno za "mining" ili rudarenje kriptovaluta. Najpopularnija i trenutno jedina priznata kriptovaluta je *bitcoin.* Radi se o virtualnoj valuti, nereguliranoj od strane vlada, te sklona promjeni tečaja s obzirom na ponudu i potražnju. Pod "priznata" se misli da se koristi za plaćanje proizvoda i usluga. Postoji preko 700 različitih kriptovaluta, no bitcoin (skraćeno BTC) je prihvaćen kao platežno sredstvo kako na internetu, tako i u fizičkim trgovinama, te postoje i BTC bankomati.

Postoje 2 načina dolaska u posjed ove valute: kupnjom, i "rudarenjem". Kupnju je moguće ostvariti uplaćivanjem određenog iznosa u nekoj od prihvaćenih "realnih" valuta, poput dolara, eura i ostalih, te se ovisno o trenutnom tečaju, dobije određeni broj BTC-a. Osim što je BTC virtualna valuta, praktički nema razlike u odnosu na bilo koju drugu valutnu konverziju, kao što bi korisnik promijenio određenu svotu dolara u euro, tako može promijeniti određenu svotu dolara u bitcoin, koji se onda nalaze u korisničkom "e-novčaniku". Time se korisniku omogućuje kupnja i trgovanje BTC valutom. Rudarenje valute podrazumijeva korištenje "minera" (rudača) valute, koji koristi računalne resurse za izračune hash tablica. Ono što razlikuje korištenje računala u mreži distribuiranog računarstva za rudarenje kriptovaluta, s ostalim projektima, jest da korisnik koji rudari kriptovalutu ostvaruje "dobit", u vidu izrudarene valute, minus određeni postotak provizije koji se daje "mreži" putem koje korisnik rudari. Rudarenje same bitcoin kriptovalute trenutno za većinu korisnika nije isplativo, te će u budućnosti biti sve manje, zbog činjenice da je maksimalan broj bitcoinova definiran, pa što je više bitcoinova na tržištu, kompleksnost njihovog rudarenja raste, te je korisnicima potrebno više vremena i više resursa za rudarenje sve manjeg broja bitcoinova. Stoga se korisnici okreću rudarenju ostalih kriptovaluta koje se u određenom trenutku više isplate, a koje je moguće zamijeniti za bitcoin. Poput svjetskih burza i valutnih tečajeva, tako postoje i burze kriptovaluta i tečaj koji varira između raznih kriptovaluta. Svi korisnici koji se odluče "stvarati" odnosno rudariti određenu kriptovalutu, ali i samo posjedovati iste, moraju imati svoj online identitet, koji im je nužan za kreiranje e-novčanika (engl. e-wallet) u kojemu će čuvati svoje kriptovalute. Isti su enkriptirani, te se i svaka transakcija kriptira, stoga je gotovo cijeli sustav "anoniman", do granice kada se odluči kriptovalutu zamijeniti za stvarnu valutu, koja je vezana za stvarnu osobu, a ne samo za online identitet. Naime, cijeli sustav korištenja bitcoin valute je anoniman, kreiran je od strane osobe ili grupe osoba pod pseudonimom Satoshi Nakamoto, no

stvaran identitet nije poznat. Od samog početka, zamišljeno je da svaka bitcoin transakcija bude anonimna, no ne i "nepostojeća", naime svaka transakcija ima svoj "hash", identifikacijski i identificirajući kod, kako bi se mogao pratiti tijek virtualnog novca. S obzirom da postoji definiran maksimalan limit bitcoinova, a ta brojka iznos 21 milijun, način praćenja transakcija onemogućuje varanje i krađu bitcoinova, odnosno krađa jest moguća, no ona ostaje zabilježena. Krađe bitcoinova se događaju, i događale su se od početka postojanja te valute. Zanimljivost oko same bitcoin valute jest upravo zabilježavanje transakcija, naime svaka transakcija se bilježi, i takav podatak je javan, što znači da svatko može pronaći svaku transakciju "svog" bitcoina, i svakog drugog. Svaki bitcoin ima svoju "adresu", te je moguće vidjeti sve transakcije određenog bitcoina sve do njegovog "stvaranja". U slučaju krađe, sama krađa je vidljiva, sa točnom adresom bitcoina, hash-a prve transakcije, hash-a transakcije kada je ukraden, te svake daljnje transakcije.[19] No sama kriptovaluta je zamišljena kao anonimna, što znači da se može otkriti samo online identitet vlasnika bitcoin-a, u ovom slučaju identitet wallet-a, a ne i neki drugi povezani online ili realni identitet. U praksi je moguće otkriti tko je vlasnik bitcoin wallet-a ukoliko vlasnik strogo ne pazi na privatnost. Naime, ukoliko se na nekom privatnom serveru, stranici ili tvrtki oglasi vlastita bitcoin adresa, moguće je pronaći tko je vlasnik servera, ili tvrtke. Nakon toga, postoji velika vjerojatno da će na vidjelo izaći i realni identitet vlasnika bitcoin wallet-a. Češći načini otkrivanja realnog identiteta jesu online kupovine, kod kojih iako je sredstvo plaćanja virtualna valuta, adresa dostave realnih predmeta jest – fizička adresa i realni identitet neke osobe. Kod ovakvih situacija, realna osoba ne mora biti i vlasnik wallet-a, ili roba može biti dostavljena u poštanski pretinac, ali šanse za otkrivanje identiteta su velike. Prilikom kupovine realnog novca sa virtualnom valutom, vrijede bankarski i ostali zakoni, što znači da, iako su bitcoin transakcije anonimne, kupovina realnog novca kriptovalutama nije anonimna, dapače, zbog zakona o spriječavanju pranja novca, svaka transakcija realnog novca povezana je sa bankovnim računom realne osobe, drugim riječima moguće je otkriti i digitalni identitet takve osobe, kao i njen realni identitet. [20]

Od ostalih projekata koje je korisno spomenuti, a koji koriste metodu distribuiranog računarstva za izvođenje analize podataka i njihovu obradu, tu su još i Einstein@home, koji se koristi za potragu signala sa neutronskih zvijezda, dakle znanstvena grana projekta jest astrofizika. Kao i kod projekta SETI@home, i ovdje postoji velika baza suučesnika, odnosno korisnika koji sudjeluju u projektu te svoje računalne resurse daju na korištenje za potrebe projekta, a takvih korisnika je oko 2 i pol milijuna, prema podacima iz 9.2015. godine [21]

19 http://www.coindesk.com/what-should-we-do-with-stolen-bitcoins/
20 https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/
21 https://einsteinathome.org/server_status.html

Zadnji ovakav projekt koji će biti spomenut jest Folding@home, a radi se o projektu u grani molekularne biologije, koji se bavi potragom za bolestima nastalima savijanjima proteina, te općenito molekularnom dinamikom. Projekt se bazira na istraživanjima Alzheimerove bolesti, Huntingtonove bolesti, raznih oblika raka te analizom virusa (prvenstveno gripe i HIV-a) i potragom za načinima njihovog spriječavanja ulaska u krvne stanice. Projekt je možda poznat i po tome da podržava i korištenje Play Station 3 konzole, koja je u vrijeme svog izlaska, omogućavala ubrzanje analize i do 20 puta u odnosu na prosječno kućno računalo iz tog doba. Projekt ima preko 8 milijuna korisnika, a po pitanju računalne moći, jedno je od najvećih, sa brzinom izračuna od okvirno 100 petaFLOPS-a. Za usporedbu, prosječno moderno kućno računalo ima moć izračuna od 1 do 4 teraFLOPS-a.

6.4. Korištenje u režimu cenzure

Osim normalnog pristupa internetu, onakvog kakvoga ga većina korisnika poznaje i koristi, te zapravo ima male potrebe za istraživanjem alternativnih metoda pristupa, u određenim situacijama korisniku se zabranjuje pristup određenim portalima, ili kompletan pristup internetu. Moguća je i djelomična cenzura, kao i pristup intranetu, u situacijama kada državni režim želi kontrolirati svoje korisnike. Može se za primjer uzeti Kinu i Sjevernu Koreju, gdje represivni organi vlasti svojim korisnicima ne dozvoljavaju pristup većini globalnih portala (uz napomenu da građani Sjeverne Koreje nemaju pravo pristupa globalnom internetu, već lokalnom intranetu sa okvirno 160 web stranica, dok je pristup "vanjskom" internetu dozvoljen samo vojnim licima i članovima višeg ranga. [22]

U Kini je situacija drugačija, pristup internetu je dozvoljen uz cenzuru svih onih portala za koje je kineska vlada donijela odluku da su "opasne", a od nedavno aktivan je zakon po kojemu bi lokalni internet provideri trebali blokirati VPN veze kojima se do sada uspješno zaobilazilo "kineski zid" - kineski firewall koji je zadužen za blokiranje i cenzuru internet prometa. [23]

Ovakvih primjera ima još, no ovo su najpoznatiji jer su najstroži. Upravo iz tog razloga, korisnici se okreću alternativnim "internetima", koji se baziraju na drugačijim protokolima, i osim što omogućuju pristup informacijama, nude i anonimnost. Većini korisnika to nije bitno, ne bave se kriminalnim radnjama, dovoljan im je osnovni pristup internetu, mogućnost komunikacije sa poznanicima, pristup lokalnim portalima, internet bankarstvu i tome slično. No vlade država, u

22 http://www.foxnews.com/tech/2017/11/10/north-koreas-internet-is-as-weird-as-think-it-is.html
23 https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html

suradnji sa lokalnim internet providerima, mogu u bilo kojem trenutku donijeti odluku da se određene web destinacije filtriraju, cenzuriraju, kao i da se kompletnim domenama zabrani pristup.

Iz tog razloga postoje projekti koji su nezavisni i nepovezani sa uobičajenim internetom, rade na potpuno drugačijim protokolima, a jedino što im treba je povezivost s krajnjim korisnikom. Takve mreže se zovu Darknet, a za pristup je u svim varijantama potreban dodatan softver kako bi se korisnika moglo povezati. Iako je pristup internetu uvjet za pristup darknetu, bitna je samo fizička povezivost, dok su protokoli nekompatibilni, te se promet u i iz darknet mreže ne vidi kao uobičajen data promet, te ga je teško ili nemoguće špijunirati. Princip rada takvih mreža je drastično drugačiji od normalnog, *world wide web* pristupa internetu. Na darknet se pristupa klijentskim softverom, sa nekoliko glavnih izbornika koji variraju ovisno o tome koju se mrežu koristi. Ono što je zajedničko darknet mrežama je veoma spor pristup, nemogućnost cenzure, i velika "dubina", što bi značilo da takve mreže imaju više slojeva pristupa, gdje je za svaki idući sloj potrebno ispuniti određene uvjete, uspostaviti veze sa ostalim korisnicima kojima se vjeruje, kako bi se moglo pristupiti i sigurnijem sadržaju. Iako u velikoj mjeri služe za razmjenu ilegalnog sadržaja, služe i raznim aktivističkim grupama za organizaciju i komunikaciju, no također i kriminalnim grupama, kao i za pranje novca , naručivanje ilegalnih stvari i usluga, planiranje političkih akcija i slično. Koliko god negativne konotacije takvih mreža bile na glasu, to je u određenim i gorenavedenim situacijama često jedini vid online komunikacije koji je moguć, ili barem koji nije praćen od strane operatera i vlasti.

Jedna od popularnijih darknet mreža jest Tor. Iako tehnički počiva na istim principima kao i druge darknet mreže, s obzirom da je popularan s velikom bazom korisnika, njegovo korištenje nije toliko enigmatično i sporo. I dalje je korisniku potreban klijentski softver, a isto vrijedi i za servere, pretraživanje tor mreže je relativno brzo u usporedbi sa klasičnim surfanjem "kroz" darknet, iz razloga što se traženi podaci nalaze unutar tor mreže. Uz malo truda može se podesiti web servere da rade isključivo unutar tor mreže, što bi značilo da nisu vidljivi ni dostupni nikome preko normalnog web-a, već korisnik mora biti spojen na tor mrežu, i znati točnu .onion adresu web servera. Onion sufiks označava da se web server nalazi u tor mreži, te mu nitko osim korisnika tor mreže ne može pristupiti. Najveći torrent trackeri imaju na tor mreži svoj backup, koje je virtualno nemoguće onesposobiti ili im zabraniti pristup, za razliku od njihovih "web" inačica koje se lako mogu onesposobiti. Ovdje vrijedi navesti da iako postoje torrent trackeri unutar tor mreže, oni služe samo za razmjenu samih .torrent datoteka, dok sadržaj nije moguće preuzimati kroz tor mrežu naprosto iz razloga što nema korisnika koji taj sadržaj "pumpaju" u tor mrežu, ali i zato jer torrent protokol nije prilagođen tor mreži. No, korištenje darknet mreža i tor-a nije samo zbog nelegalnih

aktivnosti, već je u određenim državama to jedini ili jedan od nekolicine načina kako korisnici interneta mogu koristiti svoje online identitete na globanim portalima, poput npr. Facebook-a, skype-a, i ostalih portala i servisa za online komunikaciju, sa makar djelomičnom sigurnošću da ih se neće špijunirati. Upravo u prijenavedenim državama, poput Kine, pristup globalnim servisima je blokiran, otežan ili praćen. Po podacima dostupnima na internetu,[24] Kina je blokirala svojim građanima pristup i svim google-ovim servisima, uključujući i e-mail uslugu. Među blokiranima je i facebook, youtube, twitter, dropbox, pa čak i glavna stranica Tor projekta koji je netom opisan. Upravo zahvaljujući Tor mreži, moguće je navedene servise nastaviti koristiti čak i u tom režimu nadzora i blokada, pod uvjetom da korisnik pronađe instalacijsku datotetku za Tor. Naravno da postoje i jednostavniji servisi, poput VPN-a, koji samo stvaraju tunel između korisničkog računala, i servera VPN usluge kojeg korisnik odluči koristiti, no VPN usluga i dalje počiva na standardnim protokolima i portovima koje je moguće jednostavno blokirati, a takvo je i trenutno stanje, sa više VPN servisa koji su u Kini nedostupni, odnosno veza prema VPN serveru ne prolazi prilikom pokušaja povezivanja.

Kina je u poglavlju ranije uzeta za primjer zbog toga što je njihov firewall, popularno zvan "The great wall of China", prevedeno "Veliki kineski zid", globalno poznat te često medijski praćen kada god na listu blokiranih usluga bude dodana neka nova. S druge strane postoje situacije gdje se ne može pristupiti internetu iz jednostavnog razloga što – interneta nema. Ili bolje rečeno, nema infrastrukture kojom bi se korisnici povezali na internet. Vrlo interesantan primjer je u ovom slučaju Kuba. Kuba svojim građanima ne zabranjuje korištenje interneta, no ona ga i ne nudi. Na Kubi je mrežna infrastruktura gotovo nepostojeća, a onima kojima je dostupna, je iznimno limitirana. Iako bi bilo za očekivati širokopojasne brzine pristupa, građani Kube i dalje za pristup koriste dial-up, sa bolno sporim pristupom preko klasičnih analognih modema. Niska brzina kao da nije dovoljna, nego je i cijena korištenja takve usluge toliko visoka, da prosječan građanin nije u mogućnosti platiti korištenje usluge. Ovdje na scenu stupaju "bežične točke pristupa", od engleskog izraza "wi-fi hotspots". Označavaju kutak gdje postoji bežična mreža, te se od službenog prodavača, koji radi u ime državnog telekoma, može kupiti jedan sat bežičnog pristupa internetu, po "zapadnjačkim cijenama". To bi se otprilike značilo da jedan sat takvog pristupa košta 10% mjesečne plaće prosječnog građanina Kube. [25]

Ono što je možda i očekivano za zemlju poput Kube (ili bilo koje druge sa sličnim ekonomsko-političkim režimom), jest da se velik broj građana, barem onih tehnički potkovanijih, okreće alternativnim metodana umrežavanja. Pristup internetu nije (previše) bitan, bitno je

24 http://www.businessinsider.com/websites-blocked-in-china-2015-7/#google-including-gmail-1
25 http://www.businessinsider.com/is-there-internet-in-cuba-2017-1/#increased-access-could-come-at-a-cost-11

povezivanje. Zbog toga, nastao je velik broj skrivenih mreža kojima se korisnici umrežavaju, dostupna je računalna oprema, velik broj stanovnika ima pametne telefone, te je razmjena podataka postala bitna stvar. Upravo zato, u zgradama, u kvartovima, selima i tako dalje, postoje mikro-mreže koje su korisnici sami uspostavili i koje sami održavaju, bez uplitanja države. Zajedničkim trudom, korisnici su, daleko od očiju i ušiju države, uspostavili te i dalje uspostavljaju svoje interne mreže, kabelima koje vuku po krovovima i fasadama, mrežnom opremom koju uspiju nekako nabaviti, te takve mikro-mreže međusobno povezuju još uvijek ilegalnim wi-fi linkovima, opet, opremom koju su nekako nabavili i antenama koje su sami izradili. [26]

Na takvoj vrsti "intraneta" se stroga pravila ponašanja podrazumijevaju, bilo kakva politika je zabranjena, isto vrijedi i za pornografiju, kao i za povezivanje na "vanjski" internet. Cilj ovakvih mreža je protok informacija i diljenje podataka, igranje igara, te komunikacija sa svim korisnicima. Mreža je dovoljno velika da se u njoj našlo mjesta i za vlastite web servere, chat servise, peer to peer servise, kao i društvenu mrežu. Stoga, iako u takvim mrežama ne postoji pristup "internetu" kakvim ga gotovo svi poznaju, na Kubi je to jedini način digitalne komunikacije. I o njemu ne bi bilo riječi da i ovdje ne postoje online identiteti. Svaki korisnik dobije svoje zvanične korisničke podatke kojima se povezuje na intranet. I u odvojenom svijetu poput ovoga, svaki korisnik ima svoj online identitet, iako je njegov "online" dio krajnje limitiran i malen, on postoji, i omogućuje korisnicima dovoljan broj usluga da se i oni smatraju "povezanima". Ovakvih primjera ima još, a možda su najbolji primjer razne wi-fi udruge po svijetu. U Hrvatskoj, još u vrijeme dial-up pristupa internetu, postojao je velik broj wi-fi udruga sa gotovo identičnom filozofijom postojanja – razmjena informacija, igre, komunikacija i dijeljenje podataka. I autor ovog teksta je bio član jedne riječke udruge, u vrijeme kada se brzina pristupa internetu i dalje pisala u kilobitima po sekundi, korištenje takvog oblika intraneta je imalo svoju čar i osjećaj pripadnosti određenoj subkulturi koja se ničim ne ističe. I dok , upravo na primjeru Rijeke, je bilo vidljivo više različitih subkultura, čiji su se članovi često poprilično isticali ili barem bili "vidljivi", što je u jednu ruku i logično i očekivano za grad sa takvom glazbenom scenom, korisnici wi-fi udruga se nisu ničim isticali, nisu se sastajali uživo, nisu nosili šarene irokeze i kožne jakne. Jedino po čemu ih se ponekad moglo uočiti, je bilo penjanje po terasama, krovovima i fasadama radi popravka ili montaže antene za prijem wi-fi signala udruge. I Rijeka je imala svoj intranet, uključujući i Opatiju, Lovran i ostala mjesta u blizini. No za razliku od Kube gdje su ovakve mreže jedini oblici povezivanja, u većini ostalih država je takav vid umrežavanja naprosto zaboravljen. Brzine pristupa internetu su se s vremenom drastično povećale, postali su dostupni servisi koji prije nisu postojali, a velika brzina

26 https://gizmodo.com/cubas-illegal-underground-internet-is-thriving-1681797114

prustupa je učinila da je postalo nepotrebno biti povezan u lokalnu mrežu, s vremenom je i samo održavanje opreme postalo skupo, te se udruge više nisu mogle boriti sa zastarjelom tehnologijom.

7. PRIMJER DRUŠTVE ONLINE ZAJEDNICE – PCE FORUM

Može se činiti kao ponešto zastarjeli primjer društvene zajednice, s obzirom da su forumi kao mjesto virtualnog druženja, i kao portal s izvorom informacija, kao i mjesta za traženje informacija relativno bazični, sa upitnom količinom informacija upitne točnosti, no mora se priznati da su i dalje aktualni. Naravno, to ovisi o tome kakav je sadržaj foruma, tko ga vodi, kakvi se korisnici na njemu zadržavaju i sudjeluju u radu – jer realno gledano, forum bez korisnika nije mjesto druženja, već je samo resurs koji stoji neiskorišten na nekom serveru i čeka da vlasnik servera odluči isti ugasiti.

Što se samih tipova foruma tiče, ovdje misleći prvenstveno na platformu koju se koristi, postoji poveći broj dostupnih platformi koje vlasnik može odabrati za svoj forum. Neke od tih su besplatne, dok druge koštaju određeni početni iznos za osnovnu verziju, uz doplate za "jače" verzije koje nude više opcija i mogućnosti.

Nakon pregleda dostupnih platformi, i odabira jedne na kojoj će forum biti baziran, vlasnik treba odrediti i tko će biti ciljana skupina korisnika takvog foruma. Ovdje bi se moglo razlikovati dvije vrlo široke (i nikako jedine) vrste foruma – a to je da li se radi o forumu kao vrsti *supporta* korisnicima, na primjer kompanija koja prodaje ili nudi određenu vrstu usluge i/ili proizvoda, može odabrati forum kao način davanja podrške korisnicima. Kao prednost jest – šira baza poznavaoca proizvoda , koji će pomagati ostalim korisnicima u snalaženju s uslugom / proizvodom, uz diskusiju i povratnu informaciju od strane samih korisnika, što može puno značiti ukoliko kompanija očekuje *feedback* svojih korisnika, a koji isto tako mogu savjetovati što žele ili što očekuju od proizvoda. Za razliku od podrške putem email-a, ova varijanta je kudikamo jeftinija i često brža, osobito ako postoji samo nekoliko osoba u tvrtki koji daju podršku. U ovu kategoriju bi se dalo uključiti i forume čija je glavna uloga diskusija o određenoj tematici, a koju mogu pokrenuti razni časopisi ili udruge. Popriličan broj tematskih časopisa, ali i news portala ima svoj vlastiti forum koji privlači same čitaoce takvih časopisa i portala. Iako u današnje vrijeme "brži" mediji uzimaju maha, ovdje prvenstveno misleći na facebook i lakoću puštanja komentara na određeni članak, bez da se diskusija dalje nastavlja, forumi i dalje postoje te se aktivno koriste.

Druga vrsta foruma bi bila forum vođen od strane individualca koji samo želi biti u vlasništvu foruma, a koji nije povezan sa poslovnom stranom, ne nudi support, nije orijentiran na komentiranje

specifičnih časopisa, već je njegovo postojanje samo sebi svrha. Širina pokrivenosti temama ovdje može drastično varirati ovisno o tome što vlasnik želi. Limitirajući se na hrvatsko govorno područje, jedan od foruma sa širokim spektrom tema jest forum.hr, koji sa svojim podforumima pokriva gotovo sve sfere zanimanja prosječnog korisnika. S druge strane postoje i forumi koji se bave strikno jednom tematikom ili se fokusiraju na određenu vrstu korisnika (primjer bi bio roda.hr, forum namijenjen roditeljima i onima koji će to tek postati, sa savjetima i pitanjima budućih i postojećih roditelja, o odgoju djece i svim povezanim temama). Još jedan od primjera usko-specijaliziranog foruma bi bio forum za *developere* aplikacija za mobilne operativne sustave, ovdje prvenstveno misleći na android platformu. Xda-developers forum objedinjuje 2 interesne skupine – proizvođače softvera, tj. Programere koji stvaraju nove aplikacije, i njihovi korisnici, komentirajući tako razvoj, dajući povratne informacije (engl. feedback) programerima kako bi se razvoj mogao usmjeriti ka razvoju dodatnih mogućnosti ili popraviti stare, te prijavljujući pronađene greške. S obzirom na velik spektar sličnih, ali ne istih uređaja, koji svi imaju drugačije drivere, kernele, i ostale softverske komponente, šanse da na jednom mobilnom uređaju neka aplikacija radi, a na nekom druge ne, jest nevjerojatno velika. Za razliku od iOS-a, koji je instaliran uvijek na istom uređaju – iPhone-u, kojih ima tek nekoliko različitih modela, programeri za iOS ne moraju uzimati u obzir sve moguće varijante softvera, već samo jedan – iOS. Vraćajući se na temu foruma, u RH ima svega nekoliko "popularnih" foruma. Pojam "popularni" je stavljen pod navodnike zbog subjektivnog poimanja pojma popularnog, te u ovom slučaju nije bilo istraživanja tržišta. Za potrebe ovog rada, bit će obrađen jedan specifičan forum, koji se bavi računalnom tematikom, te je to ujedno i najpotpuniji forum, s najvećom bazom korisnika na području Hrvatske. Radi se o PC Ekspert forumu, čiji je vlasnik ipak pravna osoba, radeći se o istoimenom računalnom časopisu, no i drugi poznatiji računalni časopisi dostupni u Hrvatskoj imaju svoje forume, koji su brojem korisnika manji.

Slika 12: Početna stranica PCE foruma. Izvor: autor

Autor teksta se na forum registrirao tokom 2008. godine, zbog potrebe za dobijanjem dodatnog znanja iz sfere informatike, računalne tehnike, mreža i povezanim tehnologijama. S obzirom da forum objedinjuje velik dio informatičke tehnologije kojeg kućni korisnici koriste, a

ujedno mu je to i glavna tematika, bio je dobar izvor informacija za svakodnevne informatičke nedoumice i probleme. Za razliku od raznih portala i web stranica sa opisom raznih problema i njihovim potencijalnih rješenjima, a koji se svode na seriju provjera, svodeći rješavanje probelma na metodu pokušaja i promašaja, na forumu se može postaviti direktno pitanje, te priložiti i screenshot problema, ili fotografiju, uz opis korištene opreme ili softverra. Tada slijedi rasprava od strane više i manje kompetentnih korisnika, no u konačnici pokoji dobar savjet ili točno rješenje bude napisano, te se problem riješi. Slično je i kod savjeta za neku buduću instalaciju, planiranje kupovine ili slaganje vlastitog računala, kao i kupovina novog, sa savjetima gdje, što i po kojoj cijeni kupiti ili nabaviti. Često korisnici pišu i vlastita iskustva sa određenim kupljenim komadom hardvera, dajući tako iz prve ruke svoje viđenje i svoja zapažanja, a što može uvelike pomoći ostalima koji planiraju nabaviti sličan uređaj. Ako se uzme u obzir diferencijaciju kvalitete proizvoda za istočnoeuropsko i zapadnjoeuropsko tržište, što iako nije nigdje strikno navedeno ali iz upotrebe se može zaključiti da postoji, uvelike pomaže u kupovini uređaja za kojega nema konkretnih recenzija, kao što je slučaj sa dosta uređaja koji su namijenjeni istočnoj europi. S vremenom se gradi vlastito iskustvo i znanje, čitanjem se nauči i o problemama sa kojima se još niste susreli, ali su mogući. Ostali korisnici znaju prilikom davanja savjeta i opisati što bi koji korak ili radnja značili, umjesto da se samo navede popis radnji za uraditi. Prilikom kvarova na uređajima i opremi, znaju se postaviti slike, te se iskusniji korisnici ubace sa vlastitim slikama i savjetima, a s obzirom da je hrvatsko tržište tehničke robe umjereno malo, nisu rijetki slučajevi da više korisnika foruma nabavi isti uređaj, osobito ako se čitaju recenzije te se nabavljaju best buy proizvodi.

Osim komunikacije na javnom dijelu foruma, postoje i privatne poruke, koje sliče na e-mail samo s razlikom da se umjesto e-mail adrese upisuje korisničko ime korisnika kojemu se želi poslati poruku, te vrijedi samo na tom specifičnom forumu. Razloga za privatnu komunikaciju može biti dosta, počev od toga da se ponekad forumaši sastaju uživo, kao i za međusobnu prodaju stvari poput korištenog hardvera, mobitela i slično.

S vremenom, kako član foruma "sazrijeva" i skuplja iskustvo, te odluči sudjelovati u radu zajednice pridonoseći raspravama sa korisnim savjetima i prije svega znanjem, njegova reputacija raste te , u jednu ruku, prelazi iz nevidljivog statusa juniora u status seniora, mada to nigdje ne piše niti postoji skripta koji vodi takvu diferencijaciju korisnika. Samim višegodišnjim borakvom na forumu, i bez privatne komunikacije sa ostalim članovima, već samo sudjelovanjem u raspravama, može se poprilično točno uočiti tko su iskusniji članovi, koja je njihova glavna sfera znanja i zanimanja, i tome slično, kao što se može uočiti tko su pojedinci koji svojim pisanjem ne doprinose na pozitivan način, već rasplamsavaju diskusiju burnim reagiranjem i iznošenjem dizinformacija i laži, kao što postoje pojedinci koji to rade i u realnom životu, s razlikom da su ovdje anonimni.

Prisustvo na forumu od korisnika iziskuje određeno vrijeme privikavanja, osobito korisnicima koji nisu naviknuti na takav vid društvene interakcije, bilo da se radi o korisnicima koji nisu naviknuti na društveni aspekt korištenja interneta, bilo da se radi o korisnicima koji su mlađi i naviknuti samo na društvene mreže poput Facebooka. Za razliku od službenih e-mailova, kakve bi korisnik mogao poslati određenom proizvođaču informatičke opreme ili preprodavaču, atmosfera na forumu je manje službena i više prijateljski nastrojena, no ne na razini komunikacije na društvenim mrežama. Radi se o tri potpuno drugačija oblika komuniciranja, gdje bi se moglo objasniti da je forum "u sredini" između krajnje formalne, i krajnje neformalne komunikacije. Ono što ne treba očekivati od foruma je trenutačno rješavanje upita i točan odgovor na postavljenu problematiku. Koliko god bi to moglo nekim korisnicima biti čudno, na forumima je naglasak i na tome da se svi članovi uključuju u rješavanje problema, odnosno, to se odnosi i na osobu koja traži pomoć, na njoj je da savjete koje dobije isproba te pokuša otkloniti problem sa kojim se susrela.

Konzekutivnim pridonošenjem u radu foruma i pomaganjem zajednici, što bi značilo da član redovito posjećuje forum, te gotovo svakodnevno provodi određeno vrijeme prijavljen, postoji mogućnost da ga se unaprijedi, što bi značilo da mu se dodijele dozvole koje normalni članovi nemaju, a to uključuje mogućnost uređivanja i brisanja tuđih postova i tema, "bananje" članova , što bi značilo njihovo privremeno isključivanje iz zajednice, kao i pristup zonama foruma koje nisu vidljive običnim članovima. Pisac teksta je kroz godine prošao taj proces na nekoliko domaćih i regionalnih foruma povezanih sa IT tematikom, donijelo mu je to određene usluge i konekcije, kao i određene manje materijalne nagrade, no kako se inače događa, nesuglasice u administraciji, kao i gubljenje interesa za određenu usku granu IT-a, možda i zbog napretka tehnologije i njenog mijenjanja koje pisac nije želio slijediti, danas je PCE forum jedini forum kojeg pisac redovito posjećuje. S obzirom na privatne interese, koji se djelomično podudaraju i sa poslovnim interesima, kao i time da na forumu sudjeluju članovi čija se profesija barem djelomično podudara sa planiranim kretanjem osobnog razvoja te mogu pružiti korisne savjete i znanje, za sada je PCE forum ujedno i jedini koji potpomaže privatni i poslovni razvoj pisca.

8. ZAKLJUČAK

Razvojem računala, mrežne infrastrukture, te spuštanjem ljestvice dostupnosti te tehnologije građanima, a ne više samo kompanijama, što se počelo događati već krajem 80ih godina prošlog stoljeća, mada ozbiljnije tek sredinom, odnosno krajem devedesith godina ovisno o teritoriju kojeg se promatra, pokrenut je trend, pa i potreba, za digitalnom komunikacijom i digitalnom razmjenom

informacija. Prvotno bazirani na sporim analognim vezama, koje nisu bile u stanju prenositi veće količine prometa, nastali su jednostavni servisi za online komunikaciju, poput IRC-a (skraćenica za Internet Relay Chat), putem kojih su korisnici prstupali poznatim IRC serverima i na taj način međusobno tekstualno komunicirali. Kroz samo nekoliko godina od početka korištenja interneta, dostignuta je maksimalna brzina veze moguća na analognim linijama, koja je prošla od svoje početne faze sa modemima koji su uspostavljali vezu od 4800 bita u sekundi, tj 4.8 kbita, do svoje najbrže faze koja je nudila brzinu do 56kbita u sekundi, čime se otvorio prostor da se uz tekst, šalju i slike u niskoj rezoluciji, kao i dokumenti, te je omogućilo da se korisnicima nudi veći broj usluga, poput internet bankarstva i online trgovina, unatoč maloj brzini prijenosa. Već u ovom ranom stadiju razvoja internet usluga, uviđena je potreba da se korisnike autentificira i njihov boravak na internetu, makar samo za kritične usluge – osigura i zaštiti.

Daljnjim razvojem tehnologije, analogne veze zamijenjene su digitalnima, mrežna oprema je pojeftinila, te je internet providerima postalo moguće svojim korisnicima ponuditi veće brzine pristupa internetu putem fiksne infrastrukture, a raznim zakonskim izmjenama te napretkom mobilne tehnogije, omogućilo se da se internet usluga ponudi i mobilnim korisnicima. Jednom kada su proizvođači, davaoci usluga ali i krajnji korisnici uvidjeli blagodati mobilnog pristupa internetu, uslijedio je nagli razvoj tehnologije koja je s jedne strane korisnicima pružala uslugu, a s druge strane ubrzano se počelo razvijati tržište mobilnih roba i usluga, nastali su prvi pametni telefoni, te su se putem njih počele nuditi i razne usluge, prebacujući ih, ili kopirajući ih sa fiksnih platformi (ovdje se misli na pristup računalom) na mobilne. Upravo ta mogućnost da korisnici u bilo koje vrijeme i bilo gdje da se nalazili, mogu pristupiti sve većem broju mobilnih usluga, a da njihovo konzumiranje ne košta, ili da barem ne košta previše, izazvalo je boom u korištenju i razvoju kako mobilnih usluga, tako i mobilnih uređaja. Korisnici su u masovnom broju prihvatili novu tehnologiju, koja je stvorila jedan novi stil življenja, popularno nazvan "on the go", odnosno u pokretu. U velikim gradovima, ili u mjestima gdje postoji dnevna pendulacija ljudi, mogućnost da se u vrijeme koje se troši na transport od lokacije do lokacije koristi za digitalnu komunikaciju i konzumiranje usluga, omogućila je drugačiju raspodjelu vlastitog slobodnog vremena i promijenila stil življenja. To je ubrzo dovelo do razvoja sve većeg broja povezanih usluga, u vidu usluga koje kombiniraju digitalnu komunikaciju sa realnim uslugama, pa je tako postalo moguće naručiti taxi ili sličan vid transporta na jednostavan način pomoću pametnog telefona, jednostavno pokretanjem aplikacije. Za razliku od tradicionalnog načina naručivanja taxi usluge, koje je zahtijevalo pozivanje telefonskog broja taxi servisa i objašnjavanju gdje se korisnik nalazi, danas se pomoću aplikacije može jednostavno naručiti taxi zahvaljujući GPS pozicioniranju, koje očita trenutnu lokaciju korisnika. Često se nudi i virtualno plaćanje, tj plaćanje kreditnim karticama kroz samu aplikaciju,

te korisnik ne mora niti imati papirnati novac kod sebe. Slično vrijedi i za narudžbu autobusnog prijevoza, za kojega je moguće kupiti kartu putem aplikacije, također platiti putem aplikacije, te nakon toga dobiti digitalnu kartu (u obliku 2D ili QR koda) koju onda kondukter skenira pokretnim terminalom. Plaćanje parkinga za osobna vozila je također postalo popularno razvojem infrastrukture, iako je bilo moguće od ranije kupiti parkirnu kartu putem SMS poruke, ovisno o gradu i kompaniji koja je zadužena za naplatu parkinga postalo je moguće i plaćanje aplikacijom, te se u tom slučaju naplaćuje samo cijena parkirne karte, a ne i posredovanje teleoperatera. Naime, prilikom plaćanja sms porukom, naplaćuje se i samo slanje sms poruke u visini koju je odredio teleoperater, a koja u RH iznosi 67 lipa. Korištenjem aplikacije, izbjegava se korištenje sms-a te nema naplate takve usluge. [27]

Modernih usluga ovoga tipa ima poveći broj, poput rezervacije i kupnje karata za koncerte, kino, kazalište, narudžbu u određenim servisima i plaćanja usluga, te naravno za vođenje vlastitih financija putem aplikacije matične banke kod koje korisnik ima otvoren tekući račun. Kupovina stvari putem interneta i mobilnih aplikacija je također svakodnevnica, kada gotovo svaki veći trgovački lanac ima pripadajuću aplikaciju putem koje se mogu pregledavati i naručivati artikli iz ponute, te platiti sve kroz aplikaciju, u pokretu, ne gubeći vrijeme na fizičko obilaženje trgovina. Prema istraživanju iz 2017. godine, na području Hrvatske, 85% korisnika kreditnih kartica kupuje online, dok njih 47% kupuje i u stranim online trgovinama. Po ovome, vidljiva je velika popularnost ovakvog oblika kupovanja, te se iz ovoga može logički zaključiti da vlada velika komocija, te su korisnici prigrlili mogućnost da na jednostavan, brz i nadasve fizički nezahtjevan način nabavljaju potrepštine. [28]

No, u današnje vrijeme kada je mobilna i informatička tehnologija preuzela važan dio života prosječnog građanina, koji svoje vrijeme u sve većoj mjeri prepušta digitalnoj komunikaciji, te računa na nju za obavljanje sve većeg broja djelatnosti, bitno je i da bude informiran o opasnostima koje vrebaju na internetu, kao i o potencijalnoj šteti koja može nastati uslijed gubitka kontrole nad svojim digitalnim identitetima. Gubitak kontrole ili krađa digitalnog identiteta korisnika može uzrokovati razne negativne posljedice, od onih manjih, poput gubitka vremena za pokušaj povratka ili kreiranje novog identiteta za nekritične servise, odnosno servise koji nisu previše osobno povezani sa pravom osobom, kao što to mogu biti identiteti za forume, blogove, video servise i slično, preko ozbiljnijih posljedica za servise koji na neki način prezentiraju digitalnu personu, poput linkedIN identiteta, facebook identiteta, e-mail računa, te ostalih servisa na kojima korisnik vodi svoj virtualni život ili mu barem posvećuje određeno vrijeme, do ozbiljnijih posljedica koje

27 https://www.parkingtim.hr/index.php/hr/novosti/item/park-wallet-placanje-parkiranja-putem-mobilne-aplikacije
28 http://www.netokracija.com/masterindex-hrvatska-2017-istrazivanje-138428

mogu imati i ekonomske reperkusije, poput otuđivanja kredencijala za pristup internet bankarstvu, online trgovinama koje su direktno povezane na korisnički bankovni račun, upravljanja smještajem ukoliko korisnik ima u svom vlasništvu apartmanski smještaj ili ga vodi. Ukratko, svaki oblik gubitka ili krađe bilo kojeg identiteta rezultirati će nastankom problema i njihovim više ili manje dugim pokušajima povratka. Kako se to ne bi dogodilo, korisnik mora voditi računa o sigurnosti svojih podataka, nešto čemu popriličan broj građana i dalje ne pridaju dovoljno pažnje te svoje osobne podatke ne smatra nečime što bi vrijedilo ozbiljnije osigurati, pa ih se često može naći zapisane na razne ceduljice, sms poruke, na poleđini mobitela i sličnim mjestima gdje su vidljivi većem broju osoba, ili su lako dostupni svima koji imaju pristup osobnim stvarima korisnika, te u slučaju krađe i gubitka mobitela. Lozinke za email korisnici često zapisuju na ceduljice te ih zalijepe na monitor računala, ili ih ubace u etui mobitela. Nisu rijetki ni slučajevi da korisnici zaborave svoje lozinke, te niti ne povežu dodatni e-mail račun na njega za slučaj da izgube pristup svojem primarnom e-mail računu, te niti ne vezuju svoj broj mobitela na razne servise, što se u većini slučajeva zapravo i ne preporučuje zbog zloupotrebe te informacije te preprodaje trećim stranama, koje onda na te telefonske brojeve šalju reklame i uznemiruju korisnika, no kod provjerenih providera, a osobito za e-mail račun, to je korisna mogućnost jer u kritičnim situacijama može pomoći u pristupu e-mail računu. Upravo neobrazovanost i neozbiljnost pri shvaćanju što je to digitalni identitet dovode do problema, a u moderno doba kada je sve međusobno povezano, te kada su e-usluge korištene čak i češće od realnih usluga, ozbiljnost pri čuvanju osobnih podataka bi trebao biti prioritet korisnika. Nažalost, dok se mentalitet ne promijeni, i korisnici ne počnu ozbiljno shvaćati da je i njihov virtualni identitet jednako važan kao i njihov stvarni identitet, dolaziti će do neželjenih radnji. Kroz ovaj rad opisani su glavni termini identiteta, sigurnosti, krađe podataka i socioekonomskih posljedica koje gubitak digitalnog identiteta može izazvati. Nastojalo se prosječnom korisniku približiti neke novije termine, dati uvid u problematiku održavanja i čuvanja svojih digitalnih identiteta kao i ukazati na neke propuste i ranjivosti digitalnog okruženja koje korisnik često ne uzima u obzir. Samo edukacija o e-uslugama i "digitalnom životu" mogu pomoći da se kretanje bespućima interneta učini što sigurnijim.

LITERATURA

Radovan, Mario (2016). *Communication and Control: The shaping of reality and people*. Rijeka: Mario Radovan.

Radovan, Mario (2011). *Računalne mreže 2.* Rijeka, Mario Radovan.

Pleskonjić, Dragan i ostali (2007). *Sigurnost računarskih sistema i mreža.* Zagreb: Dragan Pleskonjić, Nemanja Maček, Borislav Đorđević, Marko Carić

Benkler, Yochai (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven and London: Yochai Benkler.

Internet izvori:

Srce (2016). "Studentska iskaznica". Zagreb: Sveučilišni računski centar Sveučilišta u Zagrebu. URL: http://www.srce.unizg.hr/isak/studentska-iskaznica (zadnja posjeta 15.2.2017)

Berger, Philipp (2014). "Number of blogs worldwide". Carlsbad: Infogram. URL: https://infogr.am/number-of-blogs-worldwide (zadnja posjeta 15.2.2017)

CARNet (2013). "E-mail". Zagreb: Hrvatska akademska i istraživačka mreža. URL: https://www.carnet.hr/e-mail (zadnja posjeta 15.2.2017)

AKD (2017). "e-Vozačka dozvola". Zagreb: Agencija za komercijalnu djelatnost d.o.o. URL: http://www.akd.hr/akd/27 (zadnja posjeta 15.2.2017)

Gilad A. (2016). "Top 11 videogame & esports live streaming sites". Panama: A. Gilad. URL: http://www.thatvideogameblog.com/2016/04/05/top-11-video-game-esports-live-streaming-sites/ (zadnja posjeta 15.2.2017)

Porezna uprava (2016). "Što je OIB i zašto se uvodi". Zagreb: Ministarstvo financija, Porezna uprava, Republika Hrvatska. URL: http://www.porezna-uprava.hr/HR_OIB/Stranice/sto_je_OIB.aspx (zadnja posjeta 15.2.2017)

MUP RH (2016). "Osobna iskaznica". Zagreb: Ministarstvo unutarnjih poslova, Kabinet ministra. URL: http://www.policija.hr/42.aspx (zadnja posjeta 15.2.2017)

Todd Spangler (2016). "Younger Viewers Watch 2.5 Times More Internet Video Than TV (Study)". Los Angeles: Variety Media, LLC. (zadnja posjeta 18.11.2017)

URL: http://variety.com/2016/digital/news/millennial-gen-z-youtube-netflix-video-social-tv-study-1201740829/ (zadnja posjeta 12.1.2018)

Mike Haro (2017). " Application usage and threat report". California: Palo Alto Networks.

URL: http://researchcenter.paloaltonetworks.com/app-usage-risk-report-visualization/ (zadnja posjeta 18.11.2017)

Ernesto Van der Sar (2010). "BitTorrent Still Dominates Global Internet Traffic". USA: Van Patten Media.

URL: https://torrentfreak.com/bittorrent-still-dominates-global-internet-traffic-101026/ (zadnja posjeta 18.11.2017)

Samit Sarkar (2014). "Blizzard reaches 100M lifetime World of Warcraft accounts". New York: Vox Media inc.

URL: http://www.polygon.com/2014/1/28/5354856/world-of-warcraft-100m-accounts-lifetime (zadnja posjeta 26.11.2017)

Heike Masurek (2007). "Usage of p2p networks on the Internet". Leipzig: R&S Cybersecurity ipoque GmbH

URL: http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2007.pdf (zadnja posjeta 12.11.2017)

NASA (2017). "Pleiades Supercomputer". Washington: National Aeronautics and Space Administration

URL: https://www.nas.nasa.gov/hecc/resources/pleiades.html (zadnja posjeta 26.11.2017)

DISC (2018). “International symposium on DIStributed computing”. Massachusetts: International Symposium on DIStributed Computing.

URL: http://www.disc-conference.org/ (zadnja posjeta 13.1.2018)

Arecibo Observatory (2018). “Arecibo Observatory“. Arecibo: Arecibo Observatory

URL: http://www.naic.edu/ (zadnja posjeta 13.1.2018)

Robert Krulwich (2010). “Aliens Found In Ohio? The 'Wow!' Signal”. Washington: NPR

URL: http://www.npr.org/sections/krulwich/2010/05/28/126510251/aliens-found-in-ohio-the-wow-signal (zadnja posjeta 9.12.2017)

Danny Bradbury (2013). “What should we do with stolen bitcoins?”. New York: CoinDesk, Inc.
URL: http://www.coindesk.com/what-should-we-do-with-stolen-bitcoins/ (zadnja posjeta 9.12.2017)

Brian Booker (2018). “Top Seven Ways Your Identity Can Be Linked to Your Bitcoin Address”, Florida: 99 coins ltd.
URL: https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/ (zadnja posjeta 9.12.2017)

Fox news (2017). “North Korea's internet is as weird as you think it is”, USA: FOX News Network, LLC.
URL: http://www.foxnews.com/tech/2017/11/10/north-koreas-internet-is-as-weird-as-think-it-is.html (zadnja posjeta 13.1.2018)

Cheang Ming (2017). “China has launched another crackdown on the internet — but it's different this time”, New Jersey: CNBC LLC.

URL: https://www.cnbc.com/2017/10/26/china-internet-censorship-new-crackdowns-and-rules-are-here-to-stay.html (zadnja posjeta 13.1.2018)

Biz Carson (2015). “9 incredibly popular websites that are still blocked in China”, New York: Business Insider Inc

URL: http://www.businessinsider.com/websites-blocked-in-china-2015-7/#google-including-gmail-1 (zadnja posjeta 13.1.2018)

Harrison Jacobs (2017). “Here's what internet is like in Cuba”, New York: Business Insider Inc
URL: http://www.businessinsider.com/is-there-internet-in-cuba-2017-1/#increased-access-could-come-at-a-cost-11 (zadnja posjeta 13.1.2018)

Adam Clark Estes (2015). “Cuba's Illegal Underground Internet Is Thriving”, USA: Gizmodo Media Group
URL: https://gizmodo.com/cubas-illegal-underground-internet-is-thriving-1681797114 (zadnja posjeta 13.1.2018)

Kristijan Bečeić (2016). “PARK WALLET - Plaćanje parkiranja putem mobilne aplikacije”, Rijeka: PARKING TIM d.o.o.

URL: https://www.parkingtim.hr/index.php/hr/novosti/item/park-wallet-placanje-parkiranja-putem-mobilne-aplikacije (zadnja posjeta 21.1.2018)

Jasmina Kolić (2017). “85% Hrvata kupuje online, a beskontaktno plaća 59% korisnika kartica”, Zagreb: NETOKRACIJA d.o.o. za računalne usluge

URL: http://www.netokracija.com/masterindex-hrvatska-2017-istrazivanje-138428 (zadnja posjeta 21.1.2018)

Gary C. Kessler (2018). “An Overview of TCP/IP Protocols and the Internet”, Florida: Gary Kessler Associates

URL: https://www.garykessler.net/library/tcpip.html#evol (zadnja posjeta 21.1.2018)