Priručnik

„Zaštita digitalnog sadržaja i pojedinca u digitalnom okruženju”

Zagreb, 2018. godina

e-Škole
USPOSTAVA SUSTAVA RAZVOJA DIGITALNO ZRELIH ŠKOLA
(PILOT PROJEKT)

CARNET
znanje povezuje

Europska unija
Zajedno do fondova EU

EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI

ESF UČINKOVITI LJUDSKI POTENCIJALI

Projekt je sufinancirala Europska unija iz Europskog socijalnog fonda.

Više informacija o EU fondovima možete pronaći na: www.strukturnifondovi.hr

Sadržaj

Značenje oznaka u tekstu:

Sažetak

Digitalni mediji pružaju jednostavan, učinkovit i jeftin način razmjene informacija, stoga su postali neizostavan dio svakodnevnoga rada i odmora velikoga broja ljudi (Đurđević i sur., 2014).

Mnoštvo usluga dostupnih putem interneta od korisnika traži registraciju tijekom koje trebaju predati osobne podatke, najčešće adresu elektroničke pošte, ime i prezime. Takav način registracije očekivan je i uobičajen i ne predstavlja prijetnju korisnicima (HAKOM, 2016).

Davanje osobnih podataka kao što su prezime i ime, godina rođenja ili adresa stanovanja pri nekoj *online* prijavi je česta pojava, ali lako je moguće da pritom svoje osobne podatke odate prevarantima i tako riskirate **„krađu identiteta".** Jedan od načina na koji dolazi do krađe identiteta i način na koji se osobni podaci od nas prikupljaju zove se ***phishing*.**

Svaki korisnik interneta ima svoj digitalni ugled i identitet. On se stječe objavljivanjem raznih sadržaja ili posjećivanjem mrežnih stranica. Sadržaji mogu biti pozitivni ili negativni, a objaviti ih možete sami ili netko može objaviti umjesto vas. Svako objavljivanje sadržaja koje uključuje vas, stvara ujedno i vaš digitalni trag (Đurđević i sur., 2014).

Svaki put kad posjetimo neku internetsku stranicu na kojoj ostavljamo svoje podatke, ostavljamo i svoj digitalni trag. Zato je bitno odvojiti **privatni identitet od javnoga**. Vrlo je bitno i **zaštititi svoj identitet** jer na taj način smanjujemo digitalne tragove koje ostavljamo na internetu te mogućnost **da su na internetu dostupni sadržaji o nama koje ne želimo.**

Kako se u školama povećala uporaba IKT-a (informacijskih i komunikacijskih tehnologija), potrebno je voditi brigu o prijetnjama informacijskom sadržaju i IKT infrastrukturi koje mogu rezultirati različitim oblicima štete (npr. gubitak informacija, nemogućnost pristupa podacima i dokumentima, uništenje opreme i sl.). Zbog toga je potrebno veliku pozornost posvetiti načinima sigurnoga i odgovornog korištenja IKT-om, što je moguće postići definiranjem **Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije** te u njega uključiti **i Pravilnik o prihvatljivom i odgovornom korištenju informacijsko-komunikacijskom tehnologijom** (CARNET, 2017).

Privatnost je osnovno ljudsko pravo koja podrazumijeva trajno vlasništvo pojedinca, i označava osobne podatke u duhovnome, materijalnome, intelektualnome i kulturnom smislu. Pravila o zaštiti privatnosti u RH propisana su **Općom uredbom o zaštiti osobnih podataka, s obzirom na činjenicu da je stari Zakon o zaštiti osobnih podataka prestao vrijediti 25. 05. 2018.**

Za vrijeme pregledavanja stranica na internetu prikupljaju se naši osobni podaci. Trebali bismo znati koji se podaci prikupljaju i na koji se način upotrebljavaju.

Dokument koji se zove **Izjava privatnosti** definira načine na koje se upravlja s našim osobnim podacima i potrebno ga je pročitati prije ostavljanja osobnih podataka na nekoj internetskoj stranici.

Uvod

I davno prije ozbiljnijeg korištenja internetom susretali smo se s različitim vrstama prijevara. Ranije je to bilo bezazleno širenje „lanaca sreće“, pri čemu smo morali „pretipkati“ pismo i slati ga na desetke različitih adresa korištenjem obične pošte. Bilo je i manje bezazlenih primjera koji su mogli poprimiti elemente ozbiljne prijevare, primjerice ukoliko je uz pismo trebalo priložiti određeni novčani iznos. Iz današnje perspektive gledano, situacija je postala puno ozbiljnija i ulozi su puno veći ako ih usporedimo s onih par desetaka kuna.

Slijedom rečenog, od tadašnjih „lanaca sreće“ prošlo je puno vremena, ali je i činjenica da se kod nas, običnih korisnika interneta, nije ništa značajno promijenilo. Zapravo, ostalo je isto pa je poželjno upoznati se s rizicima korištenja interneta.

Vjerojatno ste nedavno naišli na poruku poput ove: „Sve što ste ikad objavili postaje od sutra javno. Čak i poruke koje su izbrisane ili fotografije koje nisu bile dopuštene. Facebook je sada javna osoba. Svi članovi moraju objaviti ovaj tekst kako bi se zaštitili. Ako želite, kopirajte poruku i stavite je na svoj zid. Ako ne, objavite izjavu barem jednom, to će omogućiti upotrebu vaših fotografija kao i informacija“.

Iako su naše namjere i dalje dobre i pomalo naivne te smo ovom porukom samo htjeli upozoriti prijatelje, znance i obitelj, usporedno se razvila potpuno nova „djelatnost“ – kibernetički kriminal. Kod svakog korištenja računalom, odnosno internetom, dobro je osvijestiti činjenicu kako u svakom trenutku netko želi naš digitalni sadržaj, naše osobne podatke, brojeve kreditnih kartica i sl. Također, moramo biti svjesni činjenice da kao što mi s lakoćom „dohvaćamo“ podatke s interneta, isto tako netko može „dohvatiti“ naše digitalne podatke (slike s ljetovanja, seminarske, maturalne, i diplomske radove i sl.). Pokušat ćemo smanjiti rizik od ovakvih situacija kroz primjere kvalitetne prakse postupanja s podacima.

Svi koji sudjeluju u radu na internetu, bilo to samo čitanje portala s vijestima, izloženi su riziku raznih vrsta napada koji mogu dovesti do krađe i/ili zlouporabe podataka koji se nalaze na računalu ili nanošenja štete drugim korisnicima, odnosno krađe identiteta.

U prvom se poglavlju upoznajemo s rizicima i prijetnjama u digitalnom okruženju te načinima umanjivanja prijetnji. Zbog zadanosti opsega priručnika, nisu uključeni svi rizici, samo oni s kojima se najčešće susrećemo. Koristimo se različitim uređajima, elektroničkom poštom i internetom, a budući da svaki od tih kanala komunikacije krije svoje rizike i prijetnje nužno ih je prepoznati da bi ispravno postupili.

U drugom poglavlju upoznat ćemo vas s tipovima digitalnih identiteta te mjerama njihove zaštite. Pojasnit ćemo gdje, koje i kakve informacije smijemo objavljivati te ćemo proći kroz tehnike zaštite vlastitog digitalnog identiteta.

Treće poglavlje uvodi nas u potrebu izrade „Pravilnika o sigurnoj i odgovornoj uporabi informacijsko-komunikacijske tehnologije“ na razini odgojno-obrazovnih ustanova te prikazuje dijelove Pravilnika i primjere dobre prakse. Kako bi razine sigurnosti bile pravilno postavljene, nužno je definirati krovne dokumente – politike i pravilnike.

Četvrto poglavlje uvodi nas u zaštitu privatnosti u digitalnom okruženju te se bavi njezinom zakonskom podlogom.

Priručnik je izrađen za potrebe provedbe istoimenog webinara koji se održava tijekom 2017./2018. šk. god. u okviru projekta „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot-projekt)“. Cilj webinara nije zastrašivanje korisnika digitalnih resursa (ponajprije interneta), nego stvaranje svijesti o potrebi implementiranja sigurnosnih mjera (tehničkih i kognitivnih) za smanjenje rizika vezanih uz prijetnje. Iskustvo je pokazalo kako je, uz tehničku zaštitu, edukacija korisnika ključan čimbenik u podizanju razine sigurnosti.

1. poglavlje: **Rizici i prijetnje u digitalnom okruženju**

U ovom poglavlju naučit ćete:

- ☑ koje su to izravne, a koje neizravne prijetnje
- ☑ osnove internetske sigurnosti
- ☑ o neovlaštenom korištenju osobnim podacima.

Prije nego što se usredotočimo na vrste prijetnji, važno je spomenuti kako je apsolutna sigurnost ideal koji je teško dostižan, ali na kojemu je nužno stalno raditi. Kada govorimo o sigurnosti, neizostavno je informirati se te procijeniti rizike s kojima se imamo mogućnost suočiti. Primjerice, kupujemo li putem internetske trgovine, sigurno ćemo razmisliti o tome hoće li naši osobni podaci (ime, prezime, broj kreditne kartice…) biti kompromitirani ukoliko je riječ o nekoj anonimnoj adresi, odnosno trgovini za koju nismo nikada čuli.

Jednako tako, bilo bi dobro odvojiti vrijeme kako bismo proučili i odabrali prave alate i načine zaštite. Najmanje što možemo učiniti jest podignuti svijest o prijetnjama u digitalnom okruženju te računala opremiti antivirusnim programima, ispravno konfiguriranim vatrozidom te filterom protiv neželjene pošte.

Pri odabiru načina i alata zaštite od pomoći može biti osnovno razumijevanje vrsta prijetnji koje dijelimo na:

- izravne (direktne) prijetnje
- neizravne (indirektne) prijetnje.

Neizravne prijetnje

Većina prijetnji s kojima se danas suočavamo jesu neizravne (automatizirane) i neželjene prijetnje. Ovakvim prijetnjama mi nismo cilj nego smo uglavnom kolateralna žrtva (zbog neopreznosti ili pak nedovoljno zaštićenog računala).

Bez obzira što ovakve prijetnje nisu usmjerene na nas osobno to ne znači da nam ne mogu nanijeti štetu. Primjeri neizravnih prijetnji jesu različite elektroničke poruke namijenjene krađi osobnog identiteta ili infekcije virusima. Takve su metode, u najvećem broju slučajeva, automatizirane i usmjerene na nove žrtve. Neke od metoda mogu se razviti u izravnu prijetnju, npr. ukoliko odgovorimo na obavijest o osvajanju nekog dobitka ili nasljedstva.

U neizravne prijetnje ubrajaju se i nezaštićene web-stranice ukoliko smo na njima popunili web-obrazac s osobnim podacima ili brojevima kartica. Više o ovim temama možete naučiti u ovom poglavlju.

Izravne prijetnje

Prijetnje koje smatramo izravnima puno su opasnije i izjava Brucea Schneiera, stručnjaka za računalnu sigurnost, svjedoči upravo o tome, on kaže da kako samo amateri napadaju računala, a profesionalci napadaju ljude.

Izravne prijetnje usmjerene su na nas osobno ili na našu kompaniju te uglavnom uključuju više tehnika: od socijalnog inženjeringa do različitih drugih alata. Ovakve napade često koriste ljudi koje poznajemo, odnosno ljudi koji poznaju nas, primjerice ljudi često ostavljaju datum rođenja na Facebooku koji se koristi kod „verifikacije korisničkog računa“. Njihovim iznošenjem od strane napadača, u komunikaciji s nama može se stvoriti određeni odnos povjerenja (mogli bismo pomislimo kako nas „on poznaje“), koji isto tako može biti iskorišten i u druge zlonamjerne svrhe (radi otkrivanja zaporke radi „testiranja usluge“). Takve situacije možemo smatrati izravnim prijetnjama budući smo direktno mi – privatna ili pravna osoba – „meta“ napada.

1.1 Osnove internetske sigurnosti

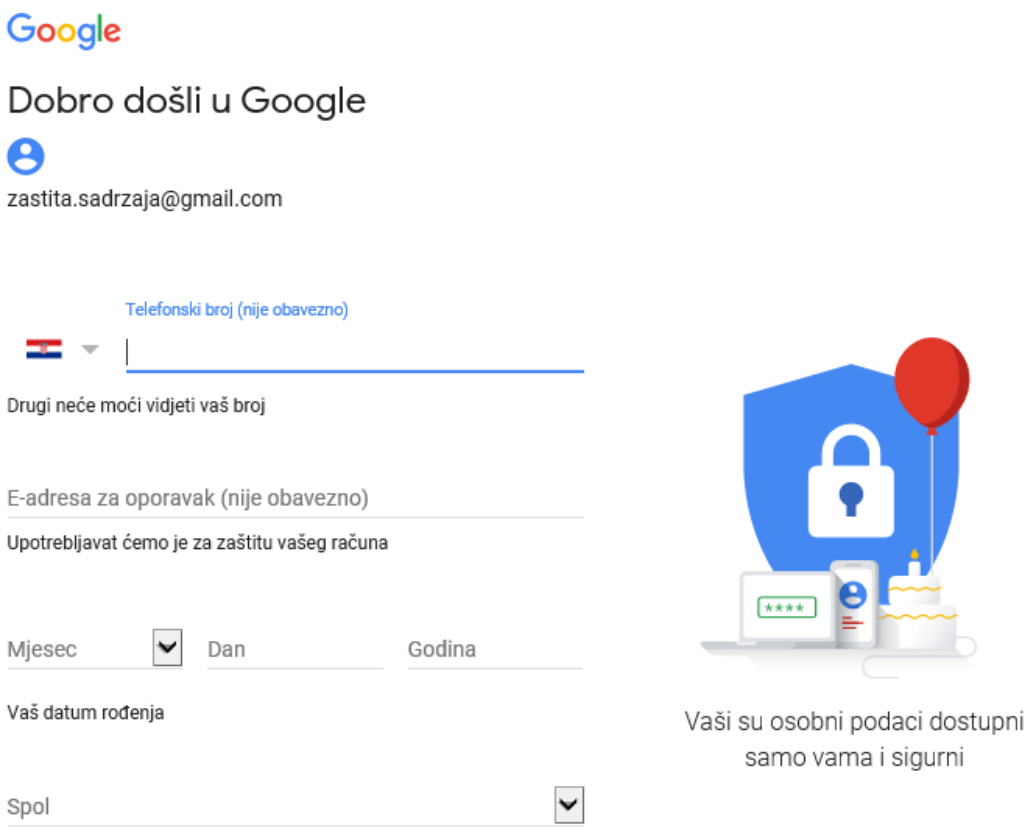
Pri radu na internetu treba imati na umu kako je proces slanja različitih poruka analogan slanju klasične pošte. Na primjer, ukoliko želimo nekome poslati knjigu klasičnom poštom, jednostavno ćemo je zapakirati i adresirati. Otprilike se isto događa i u radu na mreži, odnosno internetu, s tim da će protokol koji vodi brigu o protoku podataka na internetu i adresiranju „rastaviti“ tu knjigu na stranice. Slanje elektroničkih poruka možemo također povezati sa slanjem dopisnice – sadržaj se i u elektroničkoj komunikaciji može pročitati pa treba voditi brigu na koji način šaljemo poruke.

Budući da većinu podataka šaljemo ili putem elektroničke pošte ili putem različitih internetskih obrazaca, moramo biti svjesni kako bi takvu komunikaciju trebalo šifrirati, odnosno učiniti nečitljivom u prijenosu od našeg računala do poslužitelja i obratno.

Korištenje elektroničkom poštom

Znatan broj korisnika koristi dodatne usluge elektroničke pošte, primjerice Gmail. Pri otvaranju Google računa potrebno je upisati cijeli niz podataka – ime, prezime, zaporku, telefonski broj, dodatnu e-mail adresu za oporavak računa, dan, mjesec i godinu rođenja, spol. Kada sve ovo pročitamo na papiru, vjerojatno ćemo se zapitati je li pri otvaranju besplatne elektroničke adrese nužno upisati sve ove podatke, od kojih većinu čine osobni podaci. Nakon toga, ukoliko ste korisnik Android mobilnog telefona, uz dodavanje te adrese elektroničke pošte u e-mail aplikaciju bit ćete spojeni i na Google Play uslugu (za instalaciju dodatnih aplikacija), kao i na cijeli niz drugih usluga. Ako ste prilikom ovog procesa spajanja „brzo klikali“, a što mnogi korisnici često rade, vrlo vjerojatno ste dali i nekoliko privola za korištenje vaših podataka (za uključenje geolokacijske usluge i slično). Na temelju takvih akcija, Google posljedično onda može sakupljati podatke i pratiti što radite, što ima i svoju korisnu i svoju manje korisnu stranu. Primjera radi, uključivanje usluge lociranja omogućava pojedincu praćenje svoga kretanja tijekom mjeseca, što će mu olakšati izradu putnih naloga za poslodavca budući da korištenje ove usluge podrazumijeva sve tražene podatke na jednom mjestu. Međutim, nije problem ukoliko se korištenje ovakvih usluga svjesno odabere, problem su već spomenuta prihvaćanja postavki kao posljedica brzine i nedovoljne pozornosti, zbog čega se našim podacima mogu raditi i druge vrste obrada koje za nas nisu dio temeljne usluge, tj. usluge slanja i primanja elektroničke pošte.

Gmail usluga ima vrlo kvalitetan filter za neželjenu poštu, što nam omogućava da izbjegnemo veliku količinu neželjenog sadržaja. Također, možemo jednostavno stvoriti i dodatna pravila za filtriranje pošte. Međutim, besplatna Gmail usluga nije korporativna usluga elektroničke pošte kao Office 365 u kojemu možemo podesiti još cijeli niz dodatnih parametara, instalirati dodatne alate za provjeru sadržaja, itd. Zbog svega rečenog, korištenje CARNET webmail usluge ili usluge Office 365 za škole je nešto što je bolje prilagođeno našim poslovnim potrebama, neovisno o tome što Gmail i slične usluge koristimo kao privatne osobe.



Slika 1. Gmail usluga[1]

Elektronička pošta u sklopu sustava CARNET webmail usluge ili usluge Office 365 za škole daje nešto sigurniji način zaštite od neželjenih poruka zbog naprednog sustava filtriranja koji je zasnovan na sustavima umjetne inteligencije koji su u stanju prepoznati ih na učinkovitiji način.

Za one koji žele znati više

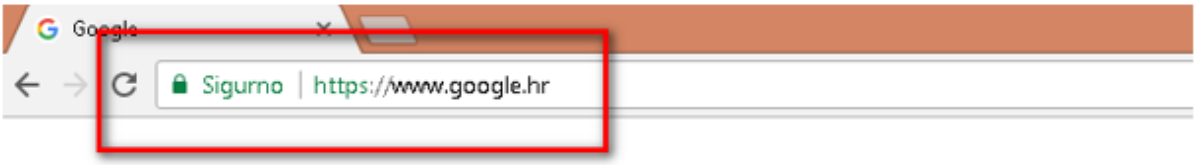
Više o sustavu Office 365 za škole pročitajte u priručniku na poveznici https://www.e-skole.hr/wp-content/uploads/2016/12/Prirucnik_Office365.pdf.

[1] https://gmail.com

Nezaštićene internetske stranice

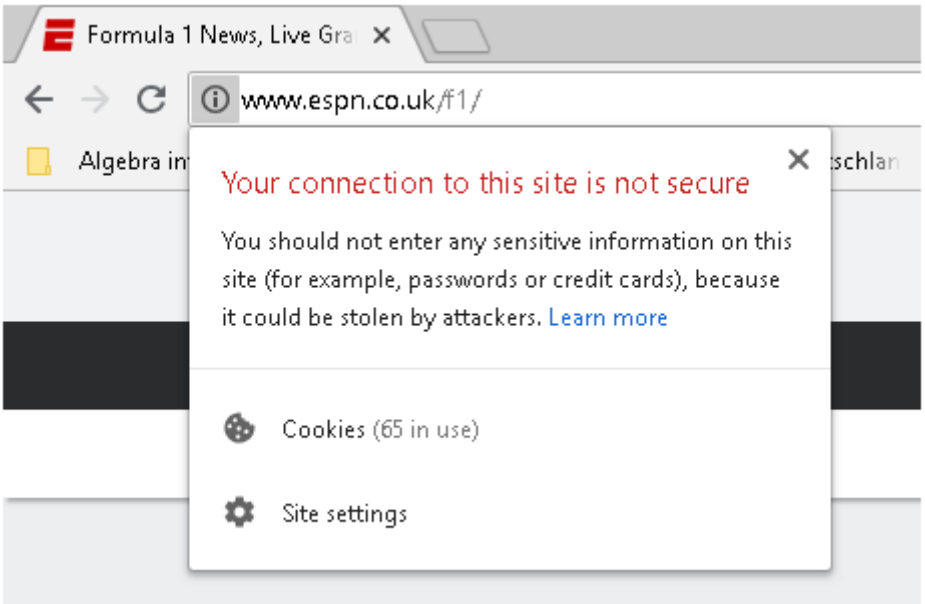
Prije nego što se posvetimo ostalim rizicima i prijetnjama u digitalnom okruženju, zadržat ćemo se na zaštićenim, odnosno nezaštićenim mrežnim stranicama.

Moguće je kako niste na to obraćali pozornost, ali od sredine 2017. Googleova početna stranica otvara se uz pomoć HTTPS protokola.



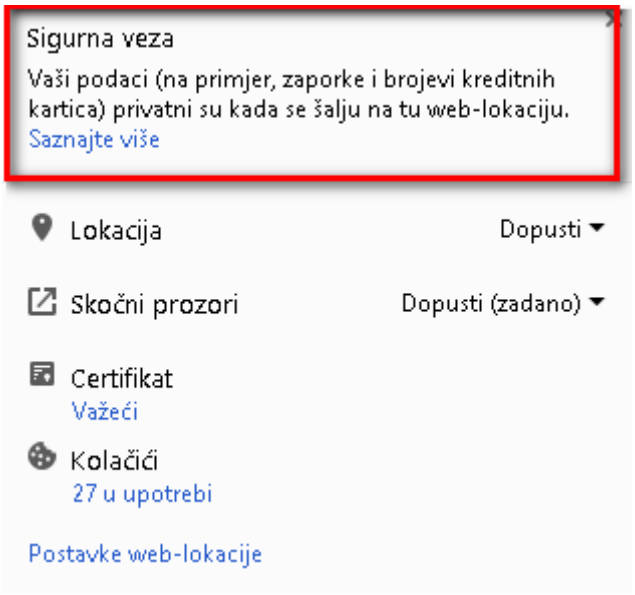
Slika 1. Internetska adresa početne stranice Google pretraživača

Vidljivo je kako uz web-adresu na koju smo se spojili putem internetskog preglednika piše **„Sigurno“.** No ako otvorite npr. www.espnf1.co.uk, slika će biti kao u donjem prikazu.



Slika 2. Početna stranica espnf1.co.uk

Kada kliknete u gornji lijevi kut stranice koja koristi HTTPS protokol, dobit ćete obavijest: „Vaši podaci (npr. zaporke i brojevi kreditnih kartica) privatni su kada se šalju na tu internetsku lokaciju.“.



Slika 3. Prednosti sigurnih veza

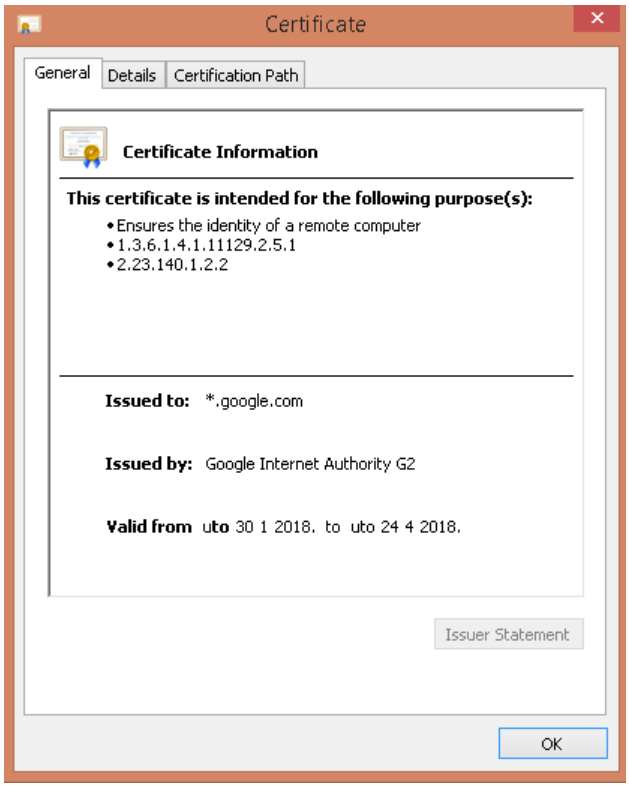
Poželjno je voditi se sljedećim principima:

1. Ukoliko pristupate internetskim lokacijama koje ne koriste HTTPS protokol, obratite pozornost na to koje podatke ostavljate, odnosno popunjavate u internetskim obrascima.
2. Nikada ne upotrebljavajte istu zaporku za više internetskih servisa, odnosno usluga, npr. za elektroničku poštu i spomenute internetske forume.
3. Ukoliko pristupate internetskim lokacijama koje koriste HTTPS protokol, provjerite dodatno adresu na koju ste se spojili, budući da je sve više napada na popularne stranice koje imaju vrlo slične adrese (npr. umjesto https://www.amazon.com, stranica putem koje se radi napad može koristiti poveznicu https://www.anazom.com).

Što znači da je veza s jednom internetskom lokacijom sigurna, a s drugom nije? Vratimo se na opis „funkcioniranja“ interneta s početka priručnika te slanje naših paketa s različitim podacima u obliku dopisnice koju bilo koji djelatnik pošte može pročitati.

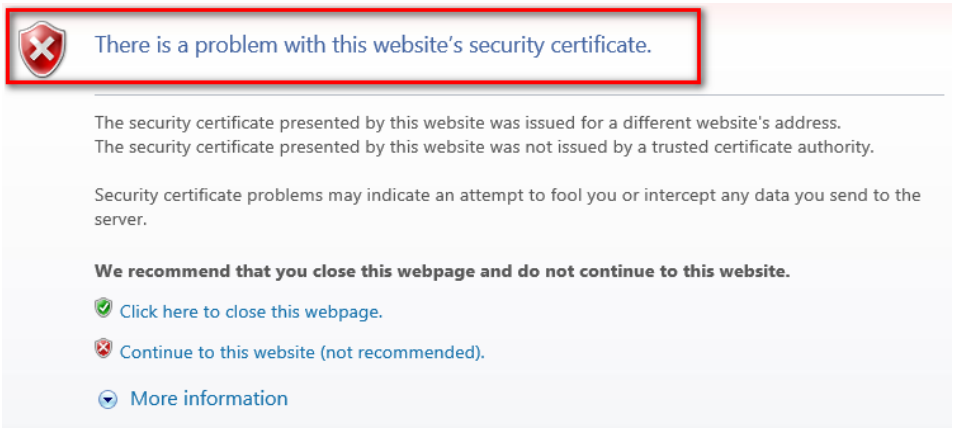
HTTP (engl. *Hyper Text Transfer Protocol*) jedan je od najčešće korištenih protokola za prijenos informacija na internetu. Osnovna je namjena ovoga protokola omogućavanje prezentacije mrežnih stranica. HTTPS je sigurna inačica HTTP protokola gdje **S** znači sigurno (engl. *Secure*), što u prijevodu znači da je komunikacija između našeg internetskog preglednika odnosno našeg računala i web-poslužitelja na koji se spajamo šifrirana. Stoga se HTTPS koristi kod transakcija prometa koji zahtijeva povjerljivost. Primjeri takvih internetskih mjesta jesu aplikacije za online bankarstvo naših banaka ili npr. internetske trgovine. Time se može postići zaštita u situacijama kada napadač pokušava prisluškivati promet u tekstualnom obliku kroz provalu u npr. komunikacijske mrežne uređaje - usmjeritelje, preklopnike i sl. U tom slučaju sav sakupljeni tekstualni promet postoje neupotrebljiv pošto se radi o prometu koji je zaštićen enkripcijom i njegova tekstualna reprezentacija nije napadaču od koristi.

S mrežnim stranicama koje koriste HTTPS protokol povezani su i digitalni certifikati.



Slika 4. Digitalni certifikat

Digitalni certifikat možemo usporediti s našom osobnom iskaznicom. U virtualnom svijetu možemo se predstavljati kako god želimo, a osoba koja se nalazi s „druge strane“ teško da to može provjeriti. U stvarnome se svijetu također možemo predstavljati kako želimo, sve do trenutka dok netko (npr. policija) ne zatraži našu osobnu iskaznicu. Policajac pri provjeri osobne iskaznice neće dvojiti u njezin sadržaj jer ju je izdao tzv. certifikacijski autoritet, odnosno onaj „kojemu se vjeruje“ (policijska uprava koja je izdala osobnu iskaznicu). Zbog svega rečenog, digitalne osobne iskaznice, odnosno digitalni certifikati, mogu biti izdani i putem mrežnih stranica, tj. poslužitelja na kojima se izvršavaju web-stranice. Poput osobne iskaznice, i certifikat ima svoju valjanost – pridružen je nekom poslužitelju, i ima svoje vrijeme trajanja. Stoga, ako na nekoj web-stranici naiđemo na upozorenje o problemu s certifikatom, nikako ne bismo trebali nastaviti koristiti to web-mjesto, a pogotovo ne unositi osobne podatke. Takvo web-mjesto treba odmah napustiti, budući da nema dokaziv „identitet“. Izuzetak bi bile situacije u kojima se interni resursi (npr. interne web-aplikacije koje koristi neka obrazovna institucija) štite sa interno generiranim certifikatima, čiji certifikacijski autoritet nije na listi certifikacijskih autoriteta kojima web-preglednici vjeruju. Naime, ne treba zaboraviti da se korištenje certifikata koji su potpisani od strane nekog poznatog certifikacijskog autoriteta obično treba platiti. Zato nam ponekad iz materijalnih razloga ne odgovara kupnja certifikata, čije se obnavljanje isto tako plaća na npr. godišnjoj razini. U tom slučaju će tehnička služba obrazovne institucije obično napraviti samopotpisani certifikat ili certifikat koji je potpisan od strane internog certifikacijskog autoriteta, zbog čega ćemo dobivati poruke kao na slici 6. U tom slučaju nema razloga za uzbunu, ali bi ovakve situacije trebale biti jasno komunicirane od strane tehničke službe prema korisnicima usluga.



Slika 5. Problemi s digitalnim certifikatom na web-stranici – preglednik nas upozorava na problem s certifikatom web-stranice kojoj smo pristupili. Uzrok je u činjenici da ime poslužitelja u certifikatu ne odgovara imenu poslužitelja na koji se spajamo ili naš web-preglednik ne vjeruje certifikacijskom autoritetu koji je izdao certifikat.

Postoji i izuzetak od ovakve dobre prakse. Često se za podizanje razine sigurnosti komunikacije na mrežnim stranicama koriste tzv. samopotpisani certifikati (*self-signed certificate*), ili certifikati koje je potpisao certifikacijski autoritet iz našeg internog IKT sustava. U tom slučaju, ukoliko smo sigurni kako se radi o našem internom sustavu (npr. neka interna web-aplikacija), možemo ignorirati upozorenje i koristiti web-stranicu neovisno o upozorenju koje nam web-preglednik daje.

Prijetnje privatnosti i identiteta

Od samih početaka ljudskog roda bilo je jasno kako s određenim informacijama treba postupati s povjerenjem. Tako je Julije Cezar još 50 godina pr. Kr. osmislio poznati Cezarov kriptografski algoritam kako bi spriječio neovlašteno čitanje poruka koje su njegovi glasnici prenosili. Informacijska sigurnost često se povezuje s računalima i računalnim mrežama, no potrebno je napomenuti da, kada govorimo o informacijskoj sigurnosti, ne govorimo isključivo o podacima pohranjenim na računalima, nego o svim informacijama koje je potrebno zaštititi od neovlaštenog pristupa, promjene ili uništavanja, bez obzira na oblik i mjesto gdje su ove informacije pohranjene.

U današnjem vremenu informatizacije, većina tvrtki i ustanova oslanja se upravo na informacijske sustave kako bi ubrzale poboljšale ili primjerice centralizirale svoje poslovanje. Odgojno-obrazovne ustanove, prateći taj način djelovanja, čine isto (Nacionalni informacijski sustav upisa u srednje škole, e-Matica, e-Imenik itd.). Odgovarajuća zaštita osobnih podataka i dalje je veliki izazov s kojim se suočavaju korisnici interneta, škole, tvrtke i državne uprave. Tehnologija istodobno može i ugroziti i štititi privatnost što, uglavnom, ovisi o načinu na koji je koristimo.

U digitalnom se okruženju treba koristiti istim postulatima kao i u fizičkom. Kao što nikada ne bismo osobne podatke dali nekome koga usputno sretnemo na ulici, isto tako treba razmišljati i kada je riječ o digitalnom svijetu. Vjerojatno je, u ovom slučaju, opasnost još i veća, budući se podaci danas mogu jednostavnije prodati ili iskoristiti za **„krađu identiteta“** no što je to bilo moguće ranije.

Vježba

Razmislite što sve znate o svom digitalnom identitetu i što činite kako biste ga zaštitili. Koje podatke objavljujete, a možda ne biste trebali?

1.2 Neovlašteno korištenje osobnih podataka

Problem neovlaštenog korištenja osobnih podataka danas je poprimio široke razmjere. Možda ste nekada primili poziv teleprodavača koji je nudio neku uslugu/proizvod, a sigurni ste da mu ne bi smjeli biti dostupni npr. vaše ime, prezime, OIB ili telefonski broj.

Kada dajemo osobne podatke, moramo biti svjesni koje smo podatke ostavili te kome smo ih dali na korištenje. Naime, svaki put kada netko dođe do, na prvi pogled beznačajnih, informacija o vama, to može iskoristiti za svoj neki cilj. Primjerice, datum rođenja čini se kao nevažna informacija, ali neke od tvrtki tom se informacijom koriste da potvrde identitet osobe koja je nazvala. Nakon što prođu verifikaciju, mogu doći do drugih informacija. Ili, na primjer, ako smo negdje ostavili broj osobne iskaznice, vrlo jednostavno možemo na web-stranici http://oib.oib.hr doći do OIB-a te uz adresu koju smo ostavili na društvenoj mreži i OIB koji smo saznali na ovaj način, kod većine teleprodavača možemo „potpisati“ ugovor na daljinu. Na ovaj način može biti učinjena i materijalna šteta.

Mnogi pružatelji usluga na internetu pri izradi korisničkih računa traže unos podataka koji im nisu potrebni, a služe za identifikaciju korisnika ako zaboravi zaporku. Primjerice, djevojačko prezime majke ne čini se kao osobni podatak, ali ukoliko smo tu informaciju iskoristili kao sigurnosno pitanje za oporavak zaporke, saznanje o prezimenu napadaču će omogućiti da pristupi vašoj usluzi te prikupi sve podatke koje ste ostavili ili pak da u vaše ime napravi neke transakcije/radnje.

Nužan je oprez i pri stvaranju novih korisničkih računa, posebice ukoliko je riječ o novim uslugama, koje globalno nisu poznate. Moguće je da je riječ o nekom lažnom servisu. Naime, napadač može pokrenuti svoju internetsku uslugu koja nudi različite pogodnosti te kroz web-obrasce prikupljati osobne podatke. Takve je servise najbolje izbjegavati ili se prije njihovog korištenja raspitati kod kolega/potencijalnih korisnika.

Budući da ne možemo utjecati na sigurnost podataka kod pružatelja usluga niti smo sigurni u njihove krajnje namjere, poželjno je da na svakoj različitoj usluzi koristimo različite zaporke i sigurnosna pitanja za njihov oporavak.

Uz neovlašteno korištenje podacima, korisnici interneta vrlo se često mogu susresti i s krađom identiteta. Kod krađe identiteta zlonamjerna se osoba koristi tuđim identitetom, lažno se predstavljajući kao druga osoba. Nerijetko je krajnji cilj vrijeđanje časti i ugleda osobe kojoj je ukraden identitet ili one koju se, uz pomoć ukradenog identiteta, napada. Namjera također može biti i realizacija nedopuštenih novčanih transakcija.

Pokušaji krađe identiteta jesu i tzv. *Phishing* poruke. ***Phishing*** (inačica engleske riječi za pecanje – *fishing*) se odnosi na prijevare kojima se služe zlonamjerni korisnici šaljući

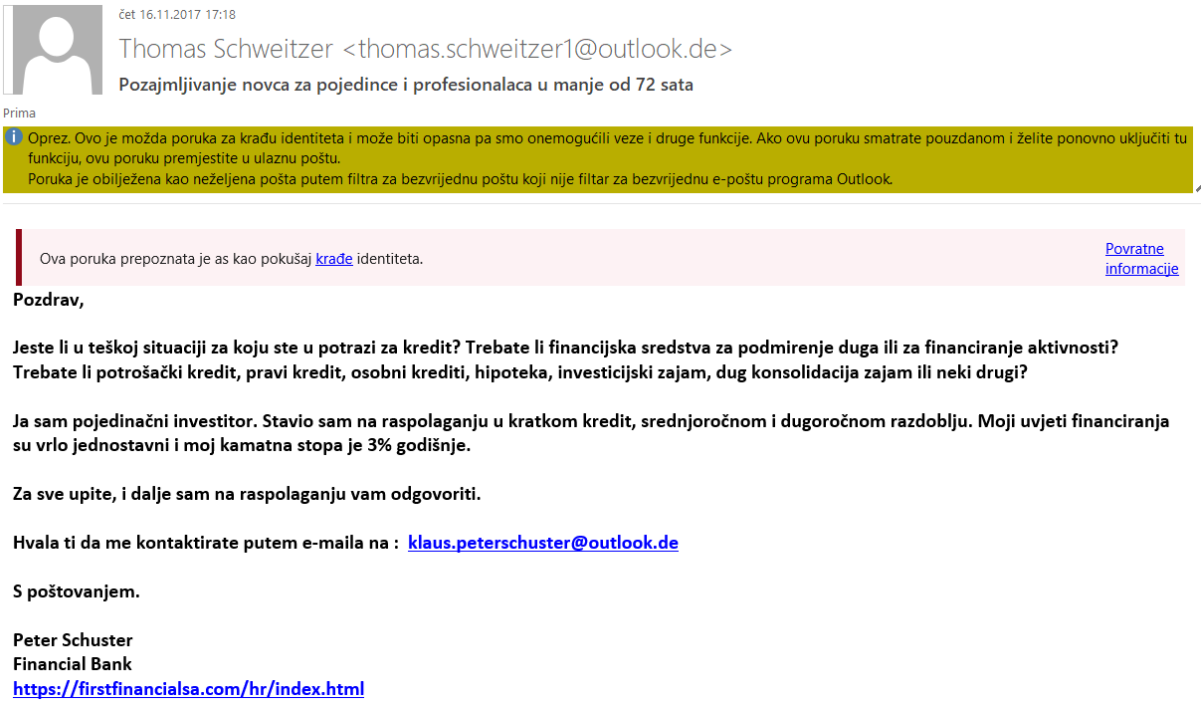
lažne poruke koristeći se pri tome postojećim internetskim servisima (Nacionalni CERT, 2016).

Phishing elektronička poruka uglavnom izgleda potpuno legitimno, ima sva obilježja kao da ju je, primjerice, poslao ugledni pošiljatelj (npr. banka, porezna uprava, kartična kompanija), a primatelja upućuje da navede svoje osobne podatke ili da posjeti web-stranicu na kojoj će ostaviti podatke. Osnovna namjera ***phishinga*** jest doći do nekog podatka koji nije javno dostupan, npr. JMBG, OIB i sl., često u svrhu ostvarenja financijske koristi.

Phishing poruke najčešće se šalju putem elektroničke pošte, a u zadnje vrijeme usmjerene su i na ostale komunikacijske kanale kao što su: forumi, blogovi, društvene mreže (jedna objava vidljiva većem broju korisnika) s nakanom i pokušajem pribavljanja podataka od što većeg broja žrtava. Najčešće takve objave budu vrlo brzo uklonjene ili se u komentarima pojavi obavijest kako je riječ o prijevari. *Phishing* poruke pojavljuju se i u aplikacijama za izravnu komunikaciju (Viber, WhatsApp, Skype i dr.) koje imaju manji domet, ali i sporiju reakciju ljudi koji se bave sigurnošću.

Popularnost ***Phishing*** napada sadržana je u činjenici kako nije potrebno veliko tehničko znanje da bi se pronašla i iskoristila ranjivost IKT opreme, budući se iskorištavaju ljudi koji nisu svjesni obmane te svojevoljno ostavljaju osobne podatke. ***Phishing*** napad počinje otkrivanjem usluga/servisa kojima se koristite (npr. u kojoj banci imate tekući račun ili kod kojeg telekom operatera imate liniju) kako bi poslana poruka bila što je moguće sličnija onima koje uobičajeno dobivate.

U *phishing* poruci vjerojatno će biti poveznica koja samo naizgled upućuje da ćemo završiti na stranici pružatelja usluga (naravno da je to varka). Ta stranica izgleda autentično te se od žrtve očekuje da unese pristupne podatke koji će završiti kod napadača.



čet 16.11.2017 17:18

Thomas Schweitzer <thomas.schweitzer1@outlook.de>

Pozajmljivanje novca za pojedince i profesionalaca u manje od 72 sata

Prima

Oprez. Ovo je možda poruka za krađu identiteta i može biti opasna pa smo onemogućili veze i druge funkcije. Ako ovu poruku smatrate pouzdanom i želite ponovno uključiti tu funkciju, ovu poruku premjestite u ulaznu poštu.
Poruka je obilježena kao neželjena pošta putem filtra za bezvrijednu poštu koji nije filtar za bezvrijednu e-poštu programa Outlook.

Ova poruka prepoznata je as kao pokušaj krađe identiteta. Povratne informacije

Pozdrav,

Jeste li u teškoj situaciji za koju ste u potrazi za kredit? Trebate li financijska sredstva za podmirenje duga ili za financiranje aktivnosti? Trebate li potrošački kredit, pravi kredit, osobni krediti, hipoteka, investicijski zajam, dug konsolidacija zajam ili neki drugi?

Ja sam pojedinačni investitor. Stavio sam na raspolaganju u kratkom kredit, srednjoročnom i dugoročnom razdoblju. Moji uvjeti financiranja su vrlo jednostavni i moj kamatna stopa je 3% godišnje.

Za sve upite, i dalje sam na raspolaganju vam odgovoriti.

Hvala ti da me kontaktirate putem e-maila na : klaus.peterschuster@outlook.de

S poštovanjem.

Peter Schuster
Financial Bank
https://firstfinancialsa.com/hr/index.html

Slika 6. Primjer *phishing* elektroničke poruke

Treba napomenuti kako nijedan legitimni pružatelj bilo koje usluge (banke, kartične kuće, telekom operateri pa čak i serviser vaše perilice rublja) od vas neće tražiti da mu šaljete osobne podatke putem elektroničke pošte.

Najčešće metode *phishinga*

- jednostavan zahtjev korisniku da (u odgovoru) pošalje svoje osjetljive podatke elektroničkom poštom, pri čemu se pošiljatelj lažno predstavlja kao npr. administrator nekoga mrežnog servisa kojemu su ti podaci potrebni radi provjere podataka, nadogradnje sustava i sl.
- lažne poveznice u porukama elektroničke pošte (obično lažna poveznica u poruci vodi korisnika na zlonamjernu web-stranicu gdje se traži da upiše svoje korisničko ime i zaporku ili druge osjetljive podatke)
- lažna mrežna stranica (korisnik može kliknuti na poveznicu koji ga vodi na web-poslužitelj koji s pomoću skripti ili funkcionalnosti web-poslužitelja izmijeni/prekrije stvarni URL svog web-sjedišta i postavi legitimni ili URL koji izgleda kao legitimni – obmanjuje se korisnika koji misli da je na legalnoj stranici, a lažna stranica prikuplja podatke dok ih korisnik unosi)
- lažni skočni prozor (*popup*) prozor na legitimnim web-sjedištima banaka – npr. „iskakanje" lažnog prozora s poljima za unos povjerljivih informacija. Lažni prozor pojavljuje se pri posjetu legitimnom web-poslužitelju (Nacionalni CERT, 2016).

1.2.1 Osnovna pravila zaštite od *phishinga* i krađe identiteta

Zaštita od ***phishing*** poruka zahtijeva educiranost primatelja. Kako napad pripada kategoriji socijalnog inženjeringa, ne postoje 100% pouzdani alati koji mogu otkriti i ukloniti takve poruke. Ipak, postoje usluge na internetu koje prate pojavu novih *phishing* poruka te poslužitelja koji ih najčešće šalju (npr.Netcraft Anti-Phisning Services, Fraudwatch International Anti-Phishing Protection Services & Solutions). Pretplatom na ovakve usluge postat ćete dio velike, globalne akcije zaštite od phishing poruka. Ukoliko je riječ o ciljanom napadu na manji broj korisnika te poruke neće biti globalno zabilježene i pružatelji usluga neće znati za njih.

Uspješnost napada možete smanjiti ukoliko se pridržavate sljedećih naputaka:

- ne odgovarajte na elektroničke poruke koje od vas traže osobne podatke
- ne otvarajte poveznice koje se nalaze unutar sumnjivih i neočekivanih poruka elektroničke pošte ili - prije nego što kliknete na poveznicu - provjerite URL koji se nalazi ispod nje te dobro provjerite odgovara li adresa stvarnoj adresi usluge
- ukoliko želite posjetiti internetske stranice s vama važnim sadržajem, nikada ne pratite poveznice iz poruka, već jednostavno unesite URL u internetski preglednik, pri čemu svakako pazite da ne zamijenite neko slovo s brojem ili obrnuto, da ne zaboravite natipkati neko slovo i slično
- ne otvarajte privitke u elektroničkoj pošti ako niste sigurni tko ih je poslao
- budite oprezni i onda kada vam poruku pošalje netko koga poznajete, jer i njegovo računalo može biti zaraženo

- uvijek provjerite odgovara li adresa mrežne stranice na koju unosite osobne podatke legitimnoj adresi (adresa krivotvorene mrežne stranice može se razlikovati i samo u jednom slovu)
- koristite se složenim zaporkama i često ih mijenjajte
- ne koristite se istim zaporkama na različitim internetskim stranicama
- provjerite koristi li mrežna stranica preko koje unosite povjerljive podatke HTTPS protokol – npr. mrežna adresa banaka trebala bi počinjati s https:// umjesto s http://
- ukoliko se komunikacija ne zasniva na HTTPS protokolu, napustite web-stranicu koja zahtijeva unošenje bilo kakvih osobnih podataka
- koristite se programom za zaštitu od neželjene pošte (anti-*spam*)
- koristite antivirusni program
- koristite *antispyware* program
- redovito ažurirajte antivirusni program te operacijski sustav koji koristite
- ukoliko primijetite ***phishing*** poruku, obavijestite stvarnu tvrtku/organizaciju koju napadač imitira, jer to može pomoći tvrtki/organizaciji u razotkrivanju napadača ali i pri njenom obavještavanju ostalih korisnika a (Nacionalni CERT, 2016).

Za one koji žele znati više

Više informacija o zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj možete pronaći na http://www.cert.hr/.

1.3 Prijevare putem elektroničke pošte

Prijevare korištenjem elektroničke pošte već su dulji niz godina vrlo popularan način djelovanja zlonamjernih korisnika, i bilo da se radi o neočekivanim novčanim dobicima ili vrlo povoljnim uvjetima kreditiranja, ponekad je dosta teško razlikovati istinu od fikcije. Problem postaje još veći ukoliko neke od ovih prijevara uključuju različite oblike kršenja vrlo „opasnih“ zakona (npr. Zakon o sprječavanju pranja novca i financiranja terorizma, Narodne Novine 108/2017), što može završiti i zatvorskom kaznom za nesretnu/prevarenu osobu koja na prijevaru nasjedne. Zbog toga ovakvim sadržajima treba prilaziti sa zadrškom, jer „ako zvuči predobro da bi bilo istinito, obično tako i jest“. Nužno je dobro upoznati najčešće prijevare i adrese na kojima se o ovakvim prijevarama možemo informirati (HAKOM, 2016).

Vježba

Razmislite koliko ste puta dobili elektroničku poštu u kojoj se od vas traži financijska pomoć ili se navodi da ste dobili novčani dobitak.

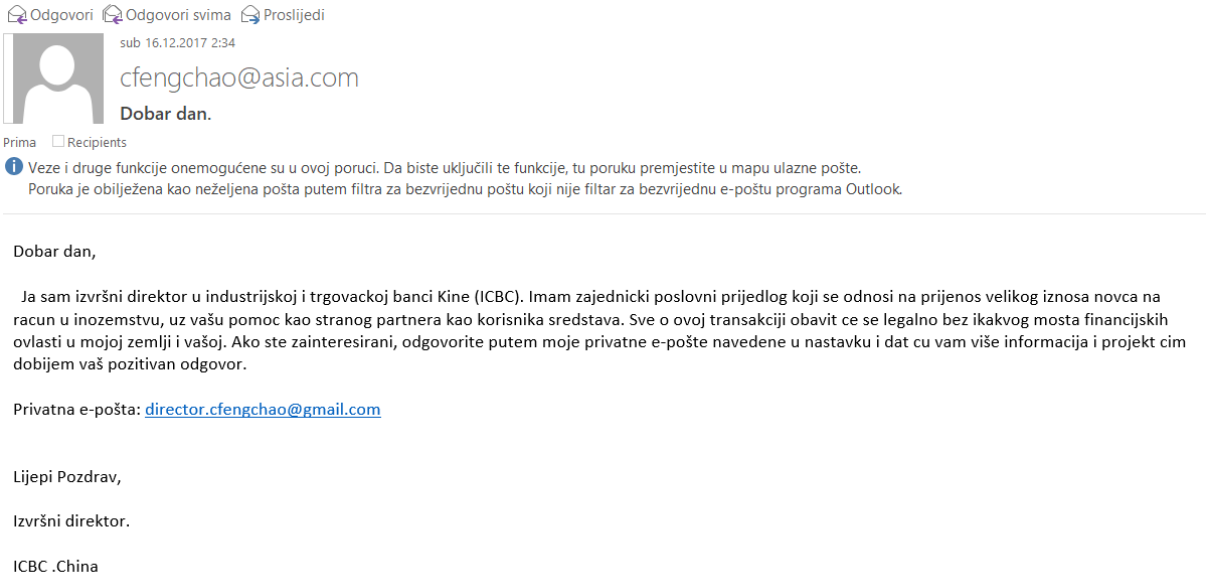
Neočekivani novčani dobici

Ovakve prijevare zasnivaju se na obavijesti o velikoj neočekivanoj svoti novca koju je žrtva osvojila ili naslijedila. Od potencijalne žrtve traži se pomoć u npr. prijenosu novca s jednog računa na drugi, jer pošiljatelj poruke to zbog različitih razloga nije u situaciji ili ne može učiniti. Obavijest se najčešće prima putem elektroničke pošte, a u novije vrijeme sve više i putem društvenih mreža (HAKOM, 2016).

Od žrtve se traži kako unaprijed mora platiti novčanu naknadu podmirenja pravnih troškova za prijenos nasljedstva iz inozemstva ili kako bi joj se mogao isplatiti osvojeni dobitak, odnosno pokriti osnovni troškovi putovanja (HAKOM, 2016).

Napadači su kreativni u izmišljanju sadržaja i pokušavaju na sve načine obmanuti potencijalne žrtve. Primjerice, tijekom 2017. svjedočili smo slučaju jedne ustanove u kojoj je djelatnicima dolazila elektronička pošta od „policije“. Poruka e-pošte upozoravala je da se ne smije odgovarati na poruke osobe X koja ukradeni novac prebacuje na tuđe račune te da će im u tom slučaju novac zaplijeniti policija. Ova poruka stvorila je predodžbu kako osoba X doista šalje novac. Nakon nekoliko dana djelatnici su dobili poruku osobe X u kojoj se nude financijska sredstva. Ukoliko bi djelatnik odgovorio na tu poruku, slijedila bi iduća u kojoj bi se tražilo da djelatnik prije transakcije pošalje sredstva za podmirenje određenih troškova.

Iako nam se ove prijevare čine očitima, lakovjernost pojedinaca, kao i nepoznavanje rizika mogu lako dovesti do problema pri korištenju digitalnog okruženja.


Odgovori Odgovori svima Proslijedi

sub 16.12.2017 2:34

cfengchao@asia.com

Dobar dan.

Prima Recipients

Veze i druge funkcije onemogućene su u ovoj poruci. Da biste uključili te funkcije, tu poruku premjestite u mapu ulazne pošte.
Poruka je obilježena kao neželjena pošta putem filtra za bezvrijednu poštu koji nije filtar za bezvrijednu e-poštu programa Outlook.

Dobar dan,

Ja sam izvršni direktor u industrijskoj i trgovackoj banci Kine (ICBC). Imam zajednicki poslovni prijedlog koji se odnosi na prijenos velikog iznosa novca na racun u inozemstvu, uz vašu pomoc kao stranog partnera kao korisnika sredstava. Sve o ovoj transakciji obavit ce se legalno bez ikakvog mosta financijskih ovlasti u mojoj zemlji i vašoj. Ako ste zainteresirani, odgovorite putem moje privatne e-pošte navedene u nastavku i dat cu vam više informacija i projekt cim dobijem vaš pozitivan odgovor.

Privatna e-pošta: director.cfengchao@gmail.com

Lijepi Pozdrav,

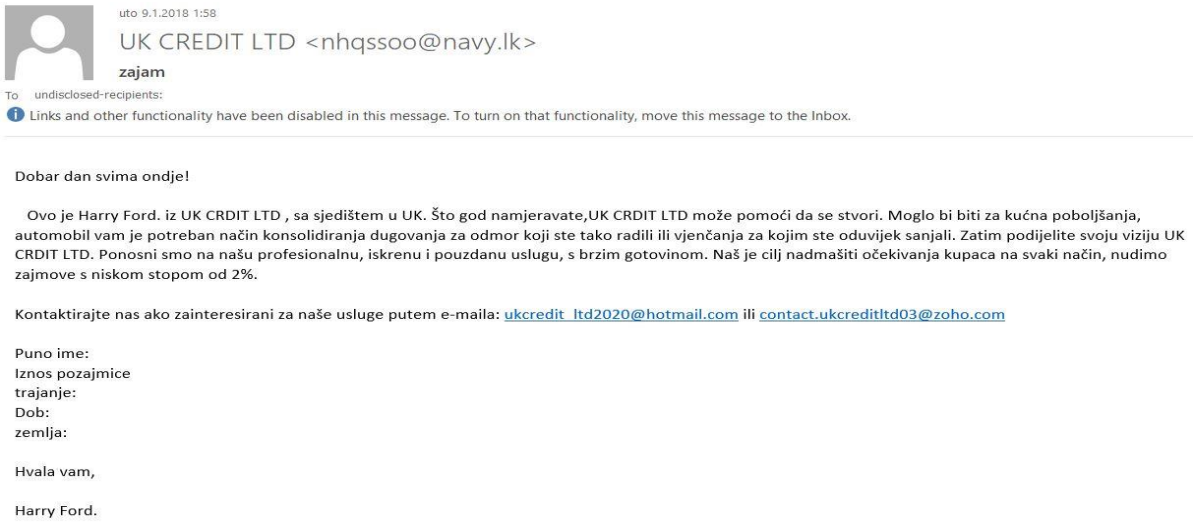
Izvršni direktor.

ICBC .China

Slika 7. Prijevara putem elektroničke pošte s novčanim dobitkom

Elektronička pošta koju šalju banke

Velika je vjerojatnost da ćete nekada primiti poruke u kojima banka ili netko u ime banke nudi različite financijske povlastice ili kredite. Čak i ako vam se netko obrati na hrvatskom jeziku ili napiše povoljno mišljenje o određenom kreditu na nekom forumu, izrazito povoljne (kreditne) ponude vjerojatno nisu vjerodostojne (Nacionalni CERT, 2016).



uto 9.1.2018 1:58

UK CREDIT LTD <nhqssoo@navy.lk>

zajam

To undisclosed-recipients:

Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.

Dobar dan svima ondje!

Ovo je Harry Ford. iz UK CRDIT LTD , sa sjedištem u UK. Što god namjeravate,UK CRDIT LTD može pomoći da se stvori. Moglo bi biti za kućna poboljšanja, automobil vam je potreban način konsolidiranja dugovanja za odmor koji ste tako radili ili vjenčanja za kojim ste oduvijek sanjali. Zatim podijelite svoju viziju UK CRDIT LTD. Ponosni smo na našu profesionalnu, iskrenu i pouzdanu uslugu, s brzim gotovinom. Naš je cilj nadmašiti očekivanja kupaca na svaki način, nudimo zajmove s niskom stopom od 2%.

Kontaktirajte nas ako zainteresirani za naše usluge putem e-maila: ukcredit_ltd2020@hotmail.com ili contact.ukcreditltd03@zoho.com

Puno ime:
Iznos pozajmice
trajanje:
Dob:
zemlja:

Hvala vam,

Harry Ford.

Slika 8. Primjer prijevare elektroničkom poštom s ponudom povoljnog kredita

Elektronička pošta u svrhu financijske pomoći ili donacija

Razlikujemo nekoliko vrsta ovakvih poruka:

- Poruke koje obavještavaju o (lažnom) dobitku na lutriji – jedan su od načina dobivanja osobnih podataka te na račun izmišljenih troškova obrade traženja uplate novca. Poruke mogu biti slane elektroničkom poštom, mogu se pojaviti u sklopu internetske stranice koju posjećujete ili na društvenim mrežama. Osim nagrada na lutriji, moguće su i druge nagradne igre, primjerice nagrada za objavu na Facebooku ili poruka da vas je Google odabrao slučajnim odabirom. Potonji načini privlačenja imaju veći učinak budući da znamo jesmo li igrali lutriju ili ne, a samim tim nije realno da dobijemo nagradu ukoliko nismo igrali. No, kao korisnici nekih popularnih servisa (npr. Google-a) možemo lakše biti zavarani informacijom da je vlasnik servisa odlučio nagraditi korisnike, među kojima smo se našli baš mi.
- Poruke koje obavještavaju o lažnom nasljedstvu – kod ovakvih prijevara napadač obavještava potencijalnu žrtvu da je od daljnje rodbine dobila nasljedstvo. Najčešće se napadač predstavlja kao odvjetnički ured te od žrtve traži da plati odvjetničke troškove i/ili naknadu koju mora platiti banci za prijenos novca na račun. Kako bi sve bilo uvjerljivije, napadač o žrtvi unaprijed sakuplja informacije putem različitih društvenih mreža.
- Lažno nagradno putovanje – kao i kod drugih prijevara, napadač obavještava žrtvu da je osvojila ili da može osvojiti nagradno putovanje. Kako bi smanjili mogućnost otkrivanja, vjerojatno će od vas tražiti da nešto učinite, primjerice: možete osvojiti nagradno putovanje u popularno odredište ako popunite neki internetski obrazac, obično upitnik. Upravo je upitnik „ključ“ za prikupljanje osobnih podataka koji se dalje mogu koristiti za manipulaciju ili pokušaj manipulacije.

- Lažne donacije – ovdje je riječ o ciljanim prijevarama koje se obično odnose na različita humanitarna događanja, npr. humanitarna kriza izazvana poplavama, potresima i sl. Ukoliko se odlučite za uplate, radite to isključivo prema naputcima i informacijama sa službenih mrežnih stranica organizacija (Nacionalni CERT, 2016).

uto 12.12.2017 2:46

Didier MUILLERMOZ <service@prodige-sender.site>

DONACIJA

Prima

Veze i druge funkcije onemogućene su u ovoj poruci. Da biste uključili te funkcije, tu poruku premjestite u mapu ulazne pošte.
Poruka je obilježena kao neželjena pošta putem filtra za bezvrijednu poštu koji nije filtar za bezvrijednu e-poštu programa Outlook.
Važnost ove poruke: Visoko.
Uklonili smo dodatne prijelome redaka u ovoj poruci.

Zdravo,
Nemam drugi način da komuniciram sa vama nego da vam pošaljem ovaj e-mail.
Ja sam u očaju i moje srce krvari dok pišem ovu poruku za koju se nadam da će vašu pažnju posvetiti.

Ja vas danas kontaktiram, jer mi je veoma tačno da ne znamo da to ne sprečava ovaj gest od mene.
Daleko sam od šala s tobom u slučaju da misliš da je to šala.
Moje ime je Didier MUILLERMOZ rođen 7. januara 1945. godine u Francuskoj i živi u Obali Slonovače.
Razlog koji me dovodi do vas je ovo:
Želio bih da prođem kroz svoj kanal da obavim dobrotvorni rad u vašem odjeljenju.

To je donacija sorti i iznosi devetsto pedeset hiljada evra (950.000 evra).
Mi bračno stanje je takvo da nemam ženu, pa čak i manje dece sa kojim sam mogao da prođe na ovom nasleđu, i ja sam trenutno boluje od raka grla terminala, ja sam osuđen na sigurnu smrt.
Zbog toga bih volio na ljubazan način i u brizi da pomognem siromašnoj deci da vam daju ovo nasledstvo da biste ostvarili ovaj posao milosrđa.

Ako se složite da uradite ono što sam vam postavio, javite mi Molimo pažljivo slušajte moj predlog, jer računam na vašu dobru volju i dobro korišćenje ovih sredstava za ovaj rad.

Hvala vam na razumevanju
Gospodin Didier MUILLERMOZ

Slika 9. Primjer prijevare elektroničkom poštom putem lažne donacije

Za one koji žele znati više

Više o prijevarama možete saznati ako posjetite **Katalog prijevara na internetu** klikom na http://privatnost.hakom.hr/catindex_hr.php.

Kako možemo prepoznati lažne poruke elektroničke pošte

Lažne poruke elektroničke pošte najlakše se prepoznaju po:

- pravopisnim i gramatičkim greškama koje najčešće nastaju pri korištenju sustava za računalni prijevod, kao što je Googleov prevoditelj
- neočekivanim porukama pružatelja usluga koje upozoravaju o brisanju, zatvaranju ili nekom drugom problemu s našim korisničkim računom
- zahtjevu da u odgovoru pošaljemo svoje osobne podatke
- sadržaju poruke koji od nas traži hitnu reakciju ili će doći do nekih posljedica
- sadržaju poruke u kojoj se nalazi samo privitak, bez dodatnog sadržaja poruke.

Spam (neželjena poruka)

***Spam* je neželjena elektronička poruka poslana s namjerom oglašavanja raznolikog reklamnog sadržaja ili u svrhu *phishing* napada te kao sredstvo širenja poveznica zaraženih virusom** (Nacionalni CERT, 2016).

Najčešće se šalje putem elektroničke pošte, ali može koristiti i druge komunikacijske alate kao što su: društvene mreže, alati za izravnu komunikaciju, forumi itd.

Osim neželjenih poruka koje sadržavaju neki vid oglašavanja, posebno su opasne one koje sadržavaju zlonamjerni kod pa na taj način pokušavaju oštetiti žrtvu.

U borbi protiv neželjenih poruka upotrebljavaju se alati i tehnike koji ih otkrivaju te na temelju korisničkih postavki odmah brišu ili spremaju u drugu mapu (neželjena pošta). Trebamo znati da svi ti alati nisu uvijek pouzdani te postoji mogućnost da će neke neželjene poruke ipak završiti u ulaznoj pošti, a legitimne pak u neželjenoj pošti.

Slika 10. Primjer neželjene elektroničke pošte (*spam*)

Kako pošiljatelji neželjene pošte prikupljaju adrese elektroničke pošte

Kako bi pošiljatelji koji šalju neželjene poruke mogli slati neželjene poruke, potrebne su im adrese elektroničke pošte. Te adrese mogu se sakupljati s različitih internetskih usluga, mogu koristiti zlonamjerne programe (viruse, crve i sl.) te sa zaraženih računala skupljati kontaktne liste ili se mogu kupiti na crnom tržištu (danas popularni DarkNet).

Najčešći način prikupljanja adresa e-pošte jest primjenom skripti koje samostalno otvaraju različite internetske stranice te s njih skidaju sve što izgleda kao adresa elektroničke pošte. Kako bi spriječili automatizirano prikupljanje, pojedini korisnici namjerno adresu elektroničke pošte upisuju s greškama. Primjerice adresu info@info.hr zapisuju s info(at)info.hr.

Adrese elektroničke pošte mogu se svrstati u tri skupine: aktivne, pasivne i obrisane (odnosno nepostojeće). Napadači koji šalju neželjene poruke žele slati poruke samo na aktivne adrese. Obrisane ili nepostojeće adrese nije problem prepoznati jer će nam poslužitelji elektroničke pošte javiti da je primatelj nepoznat, ali što je s pasivnim adresama? Gotovo svatko od nas ima neku adresu elektroničke pošte

koju ne koristi već godinama ili je nikad nije ni koristio. Primjerice, praksa pružatelja usluga pristupa internetu u Hrvatskoj jest da nakon sklapanja ugovora pružaju i „poštanski sandučić“. Takve se adrese većinom uopće ne upotrebljavaju. SPAM poruke poslane na takve adrese u pravilu nitko ne čita.

Kako bi došli do aktivnih adresa e-pošte, napadači najčešće unutar poruke dodaju poveznicu preko koje se možete odjaviti te više ne primati poruke. Naravno, klikom na tu poveznicu napadaču ste potvrdili da se adresa e-pošte upotrebljava te da je netko pročitao poruku.

Savjeti za zaštitu od neželjene pošte

Potpuna zaštita od neželjene pošte teško je ostvariva, budući je elektronička pošta postala gotovo primarni oblik komunikacije kako u poslovne tako i u privatne svrhe. Ukoliko prilagodite *SPAM* filtar da svu poštu koja dolazi s adresa koje nemate u kontaktima proglasi neželjenom, otvaraju se dva problema: prvi je da nećete moći primiti poštu ni od koga ako nije na vašem popisu kontakata, a drugi je da svejedno možete dobiti neželjenu poruku, i to ako je šalje netko koga poznajete, s računala zaraženog zlonamjernim programom.

Jedan od dobrih načina zaštite od neželjenih poruka je prelazak na sustav elektroničkih poruka u sklopu sustava Office 365 za škole. U pozadini *spam* filtera nalazi se sustav umjetne inteligencije koji prati elektroničku komunikaciju na razini velikog broja korisnika te dinamički kreira pravila za filtriranje neželjenih poruka.

Savjeti za smanjenje broja neželjenih poruka koje primate jesu:

- ne objavljujte adresu elektroničke pošte na javno dostupnim mjestima kao što su društvene mreže, forumi, *news* grupe ili sl.
- ako trebate objaviti adresu jer želite da vas preko nje kontaktiraju, probajte ju zapisati u obliku koji će automatiziranim skriptama otežati prepoznavanje, npr. info**at**carnet.hr, pri čemu smo znak @ zamijenili s at. ili maknipriješlanjanamailinfo@carnet.hr
- ne pretplaćujte se na *mailing* liste koje šalju obavijesti o besplatnim uslugama i novim proizvodima
- ukoliko želite primati obavijesti s *mailing* lista, najbolje je da napravite dodatnu adresu elektroničke pošte ta da se njome koristite na internetskim stranicama koje nude usluge slanja obavijesti ili od vas traže adresu radi slobodnog preuzimanja nekog sadržaja
- ne koristite se poveznicama za odjavljivanje s lista ako se ne sjećate da ste se na tu listu pretplatili (napravite pravilo za snimanje takvih poruka u mapu „Neželjena pošta“)
- kreirajte filter u svom programu za rad s elektroničkom poštom koji će neželjene poruke preusmjeravati u za to kreiranu mapu (Nacionalni CERT, 2016).

Za one koji žele znati više

Izrada privremene adrese elektroničke pošte moguća je na internetskom servisu https://www.crazymailing.com/hr/.

Kako zaštititi djecu i mlade od krađe identiteta

Djeca su često izložena riziku krađe identiteta zbog neiskustva i nedostatka opreza. Ne postoji tehnička zaštita koja može osigurati sigurnost pa je zato edukacija iznimno bitna. Djecu moramo upozoriti o ugrozama koje postoje i posljedicama koje mogu nastati neopreznim ponašanjem. Prije nego što im dopustimo korištenje neke usluge, trebali bismo naučiti postaviti zaštite privatnosti (najbolje zajednički, kako biste tijekom prilagođavanja postavki objasnili važnost), zatim im objasniti koje osobne podatke smiju dati kada se koriste internetom te koje podatke smiju dati osobama koje ne poznaju, pojasniti da svoje pristupne podatke ne smiju dati nikome (osim roditeljima), uputiti ih da vode brigu o tome što objavljuju jer njihove objave (*postovi*) zauvijek ostaju na internetu te mogu prouzročiti štetu njima ili okolini. Bitno je da znaju da ne smiju ostavljati ni osobne podatke drugih jer na taj način narušavaju njihovu privatnost. Dodatno, djeci je potrebno detaljno objasniti što trebaju poduzeti i koga kontaktirati ukoliko se dogodi nešto neočekivano ili sumnjivo u njihovoj digitalnoj okolini.

Što učiniti u slučaju zlouporabe osobnih podataka ili krađe identiteta

Nužno je odmah reagirati i slučaj prijaviti policiji uz navođenje svih relevantnih činjenica i dokaza koje ste u mogućnosti priložiti. Ukoliko je riječ o: primjerice lažnim ugovorima, nužno je odmah o tome obavijestiti pravnu osobu s kojom je ugovor sklopljen (AZOP, 2016).

Budući da je riječ i o povredi Uredbe o zaštiti osobnih podataka, može se podnijeti zahtjev za zaštitu prava Agenciji za zaštitu osobnih podataka (AZOP, 2016).

1.4 Prijetnje pomoću društvenih mreža

„Osim što su uvelike promijenile način komuniciranja i povezivanja putem interneta, društvene mreže utječu i na naš svakodnevni život. Internet je omogućio da jednostavno pratimo čime se bave naši prijatelji, dopisujemo se s njima putem poruka ili chata, postavljamo albume fotografija, glazbu koju volimo, igramo igre u kojima možemo kupiti virtualne predmete, pretplaćujemo se na praćenje obavijesti na profilima poznatih osoba ili političkih stranaka, biramo koga želimo pratiti više, a koga manje itd“ (CARNET, 2013: 2).

Društvene mreže omogućuju otvaranje profila bez provjere identiteta te zadovoljavanje potreba korisnika da se prikažu točno onakvima kakvima žele da ih ostatak korisnika na društvenim mrežama vidi.

Masovno korištenje društvenih mreža privuklo je i napadače koji ih vide kao medij za svoje zlonamjerne aktivnosti. Društvene mreže im omogućuju brzo širenje zlonamjernog sadržaja, a pritom osiguravaju određenu vjerodostojnost, jer korisnici vjeruju svojim prijateljima (CARNET, 2013).

Nažalost, sve većim rastom broja korisnika društvenih mreža raste i broj kriminalaca koji, djelujući na njima, žele ostvariti financijsku ili drugu korist. Takvi zlonamjerni postupci imaju za cilj krađu svih osobnih podataka do kojih je moguće doći. Korisnik zbog toga može pretrpjeti krađu identiteta ili financijsku štetu.

„Napadači se za širenje zlonamjernog sadržaja koriste lažnim reklamama (uključujući i oglase koje napadači legalno kupe), promocijama, aplikacijama i personaliziranim porukama. Pritom, putem **socijalnog inženjeringa** pokušavaju manipulirati korisnicima koristeći se njihovim emocijama te ih nastojeći navesti na otvaranje zlonamjernog sadržaja“ (CARNET, 2013:3).

Sadržaji koje napadači objavljuju na društvenim mrežama često vode na neke druge, zlonamjerne URL adrese koje su u pravilu zadužene za zarazu računala korisnika.

„Korisnici društvenih mreža se tako najčešće mogu zaraziti putem:

- poveznica u statusima prijatelja
- privatnih poruka
- poruka na *chatu*
- zlonamjernih URL-ova na grupama, profilima poznatih ličnosti“ (CARNET, 2013:3).

Socijalni inženjering posebna je kategorija napada koja se ne temelji na tehničkim ili sigurnosnim ranjivostima, već na mogućnosti obmane, odnosno manipuliranja ljudima u svrhu provođenja aktivnosti koje napadač želi ostvariti . Govoreći o napadima socijalnim inženjeringom, zapravo se najčešće govori o nekim vrstama prijevara koje su zasnovane na dobro osmišljenim scenarijima kako bi se osobu koji ima pristup nekim informacijama navelo da npr. te informacije svojevoljno preda napadaču (Nacionalni CERT, 2016). Ključna značajka napada socijalnim inženjeringom je upravo ta da žrtva svojevoljno provodi neku aktivnost – napadač ju je uvjerio da je riječ o bezopasnoj aktivnosti koju treba ostvariti iz određenog razloga.

Socijalni inženjering najčešće se koristi za otkrivanje povjerljivih informacija ili dobivanja pristupa nekim drugim resursima do kojih napadač inače ne bi mogao doći.

Za one koji žele znati više

Više o socijalnom inženjeringu možete pronaći na linku http://www.cert.hr/socijalni_inzenjering.

Oblici prijetnji na društvenim mrežama

Vježba

Razmislite koliko ste sigurni da putem društvenih mreža uvijek komunicirate s osobama koje poznajete.

Kako Facebook ne daje informacije o korisnicima koji su pogledali vaš profil, a to je zanimljivo većini korisnika i željeli bi znati tko je sve gledao njihov profil, napadaču je cilj napraviti Facebook aplikaciju koja korisnicima omogućuje uvid. Naravno, većina korisnika odmah pokrene aplikaciju koja napravi neku štetu. Slična je prijetnja i lažna aplikacija koja pokazuje tko je gledao vašu vremensku crtu (engl. *Timeline*).

Česte su i prijevare putem poveznica sa zastrašujućim ili smiješnim videozapisima i fotografijama pokraj kojih se pojavljuju čudne poruke. Kada korisnici kliknu na tu poveznicu, poruka se pojavljuje na vremenskoj crti i na taj se način širi dalje.

U posljednje su vrijeme sve učestalije prijevare koje se odnose na besplatno dijeljenje proizvoda ili bonova. Žrtve koje su kliknule na poveznicu i ispunile obrazac zapravo su pristale na primanje skupih SMS poruka. Primanje tih poruka jako je teško zaustaviti.

Načelo prijevare vrlo je jednostavno. Napravljena je mrežna stranica na kojoj je kratka anketa koju bi korisnik trebao ispuniti kako bi dobio mogućnost osvajanja nagrade/bona. Nakon što ispuni anketu, korisnik bi informaciju o nagradi trebao podijeliti na društvenoj mreži sa svojim prijateljima.

Dijeljenjem poveznice i „lajkanjem“ stranice (koja se predstavlja kao stranica tvrtke), korisnici zapravo izlažu svoje osobne podatke riziku i krađi identiteta. Također, može im se dogoditi da na svoj profil počnu dobivati čudne poruke i oglase.

No, ove radnje mogu biti i puno ozbiljnije. Korisnici nisu ni svjesni koliko osobnih podataka zapravo pohranjuju na računima društvenih mreža – od punog imena i prezimena, grada u kojem žive, adrese elektroničke pošte, broja mobilnog telefona itd.

Savjeti mladima o ponašanju na društvenim mrežama

Mladi su izrazito ranjiva skupina jer ponekad, naročito u brzini - ne razmišljaju o posljedicama svojih radnji. Radi sigurnijega korištenja internetom važno ih je educirati da:

- razumiju osnove sigurnosti i privatnosti na internetu
- informacije koje ostavljaju o sebi i drugima mogu puno govoriti o njima i pomoći u krađi identiteta
- ne daju nikome svoje korisničke podatke (zaporke) – ni najboljim prijateljima ili mladiću/djevojci te da ih čuvaju od krađe. Osobe koje saznaju njihovo korisničko ime i zaporku mogu u potpunosti izmijeniti sadržaj profila na društvenim mrežama
- koriste postavke privatnosti na profilima društvenih mreža
- ne objavljuju podatke o svojim prijateljima ili drugim osobama bez njihova pristanka
- prije kreiranja korisničkog računa na nekoj internetskoj stranici pročitaju pravila ponašanja i upoznaju se s informacijama o prijavljivanju neželjenih sadržaja.

Savjet

Pročitajte pravila o korištenju osobnim podacima na Facebooku:

https://www.facebook.com/privacy/explanation.

Ako želite ukloniti svoje osobne podatke s društvenih mreža, podnesite zahtjev na stranicama AZOP-a:

http://azop.hr/zahtjevi-za-uklanjanje-osobnih-podataka/%22.

1.5 Savjeti za zaštitu računala i podataka[2]

Ne otvarajte poruke e-pošte nepoznatih pošiljatelja

Ako dobijete e-poštu od nepoznate osobe, trebate biti oprezni jer katkad i samo otvaranje poruke može zaraziti vaše računalo, a posebno ako napadač zna za neku ranjivost u programu kojeg koristite za rad s e-poštom. Jednako tako, trebate biti oprezni kod korištenja privitaka koji se nalaze u porukama. Ako vam je nešto sumnjivo u poruci ili privitak ne očekujete, možete ga provjeriti na stranici https://www.virustotal.com/hr/.

Koristite antivirusni program

Obvezno na računalu instalirajte antivirusni program. Ukoliko je riječ o osobnom računalu, na tržištu postoji veliki broj besplatnih programa koji će spriječiti većinu napada. Ako je pak riječ o poslovnom računalu, onda tvrtka/organizacija u kojoj radite treba kupiti antivirusni program. Ti su programi vrlo efikasni u pronalaženju i uklanjanju virusa i drugih zlonamjernih programa koji pokušavaju zaraziti vaše računalo. Više o virusima i ostalim vrstama zlonamjernog koda možete naučiti u webinaru Rješavanje problema prilikom korištenja i korištenjem digitalne tehnologije te u istoimenom priručniku dostupan na web-stranici pilot-projekta e-Škola (https://www.e-skole.hr/hr/rezultati/obrazovanje-i-podrska/obrazovni-sadrzaji/).

U internetskom pregledniku upotrebljavajte blokator skočnih prozora

Prilagodite svoj internetski preglednik tako da blokira skočne prozore (*pop-up*). Iako većinu tih prozora stvaraju oglašivači, oni mogu sadržavati i zlonamjeran program. Blokator skočnih prozora može spriječiti prikaz takvih prozora. Te će postavke u nekim slučajevima spriječiti i legitimne aplikacije, ali uvijek imate opciju da za pojedine internetske adrese napravite iznimku.

Savjet

Upute o blokiranju ili onemogućavanju skočnih prozora u web-preglednicima možete pronaći ovdje:

Google Chrome – https://goo.gl/phUwbt

Mozilla Firefox – https://goo.gl/WFn66Y

Microsoft Edge – https://goo.gl/twqNAn

Safari – https://goo.gl/7AoS1Q.

Redovito ažurirajte operacijski sustav

Proizvođači operacijskih sustava redovito izdaju sigurnosna ažuriranja koja pridonose sigurnosti računala. Ispravljanjem sigurnosnih propusta, ova ažuriranja sprječavaju zarazu virusima i druge napade putem zlonamjernog programa. Redovito ažuriranje jako je bitno jer napadači ažuriranje mogu analizirati odmah po njegovu izlasku te ga probati iskoristiti na svim računalima koja nisu ažurirana.

---

[2] Prilagođeno prema Preventivnim mjerama zaraze navedenima na stranicama Nacionalnog CERT-a: http://cert.hr/malver/savjeti.

Koristite se vatrozidom

Vatrozid *(*engl*. Firewall)* je program kojim se kontrolira mrežni promet te ga, ovisno o postavkama, odbacuje ili propušta. Vatrozid poboljšava zaštitu računala i sprječava nedopušteni pristup putem mreže ili interneta.

Savjet

Različite vatrozidove možete pronaći na linku:

https://goo.gl/wDFVdD.

Koristite se postavkama zaštite privatnosti internetskog preglednika

Neke mrežne stranice mogu pokušati iskoristiti osobne podatke radi prijevare i krađe identiteta. To možete spriječiti ako pregledniku zabranite korištenje osobnim podacima. Pri posjećivanju neke od stranica za koju niste sigurni možete se koristiti novim prostorom s uključenom zaštitom privatnosti. Ovo je dobra mogućnost i pri pretraživanju interneta s tuđih računala.

2. poglavlje: **Digitalni identitet**

U ovom poglavlju naučit ćete:

- ☑ što je digitalni identitet
- ☑ što sve internet zna o vama
- ☑ kako zaštititi svoj identitet i osobne podatke na internetu.

Budući se često moramo prijaviti na različite informacijske sustave, npr. e-dnevnik, prijavom obično prolazimo dva koraka, autentikaciju i autorizaciju.

„Autentikacija (engl. *Authentication*) je proces kojim se na temelju danih podataka korisnik identificira odnosno potvrđuje se njegov identitet. Danas najrasprostranjeniji način identifikacije korisnika jest korisničko ime i zaporka koji su sastavni dio korisničkog računa odnosno digitalnog identiteta“ (Car, Kralj, 2016).

Privatni elektronički identitet predstavlja identitet koji vam je dodijelila organizacija, odnosno ustanova u kojoj ste zaposleni.

U Republici Hrvatskoj korisnici iz ustanova članica CARNET-a (učenici, nastavnici, studenti, profesori, znanstvenici i zaposlenici ustanova članica) dobivaju elektronički identitet u sustavu **AAI@EduHr**. To je virtualni identitet koji im omogućuje korištenje CARNET-ovih, kao i drugih usluga (e-Građani, eduroam, eduGAIN, AAI PKS, i sl.) Jednako tako,s obzirom na pouzdanost i važnost sustava AAI@EduHr, korisničko ime i lozinka iz sustava AAI@EduHr može se koristiti i za pristup usluzi e-Građani.

Privatni elektronički identitet u sustavu AAI@EduHr ima oblik ID_korisnika@oznaka_ustanove.hr, npr. ime.prezime@skole.hr.

Elektronički identitet vlasniku identiteta često omogućava da pristupa većem broju usluga putem SSO-a (engl. *Single sign on* – jedinstveni prijavni sustav), svojim osobnim podacima te da ostvaruje različita materijalna prava. Zbog svega navedenog, elektroničkim se identitetom treba koristiti isključivo osobno i nikad ga ne treba dijeliti s drugim osobama.

„Elektronički identitet u sustavu AAI@EduHr potrebno je imati za korištenje većeg broja usluga spajanja na internetsku mrežu, pristupa računalnim resursima te prijavu na velik broj web-aplikacija kao što su npr. sustavi za udaljeno učenje, *online* baze podataka itd. Pripadnici akademske i istraživačke zajednice u Republici Hrvatskoj elektronički identitet u sustavu AAI@EduHr mogu zatražiti i dobiti isključivo u nadležnoj matičnoj ustanovi, a elektronički identitet im može dodijeliti samo ovlaštena osoba, tzv. administrator LDAP imenika ustanove“ (Srce – Sveučilišni računski centar Sveučilišta u Zagrebu, 2017).

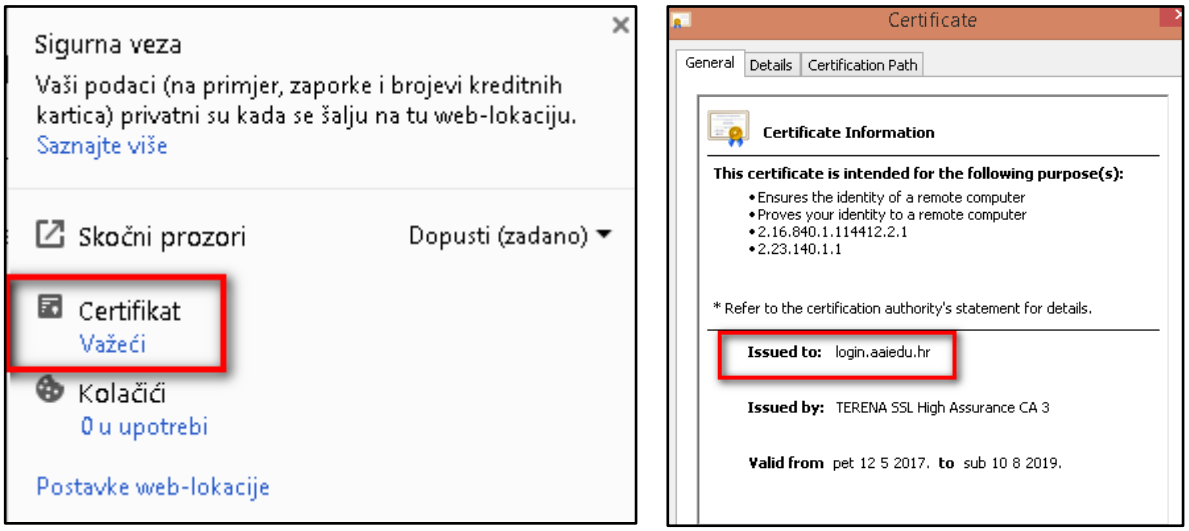
Bitno je da ga zaštitimo sigurnim zaporkama kako ne bismo postali žrtva krađe identiteta. Korisnički račun obvezno mora imati dodijeljenu zaporku. Zaporka može biti prazna, no takav pristup nije preporučljiv, zbog sigurnosnih razloga. Također, preporučuje se koristiti složenije zaporke koje nije lako pogoditi.

Korisnike treba educirati o opasnostima i prijetnjama za računalni i informacijski sustav koje vrebaju ukoliko zaporke nisu postavljene ili ih je moguće lako pogoditi.

- Opasno je koristiti se zaporkama s očitim asocijacijama kao što su npr. prezime ili datum rođenja
- Zaporke veće duljine teže je pogoditi. Maksimalna duljina zaporki je 127 znakova, a nije preporučljivo koristiti zaporke kraće od 8 znakova
- Ne koristiti riječi iz rječnika bilo kojeg jezika, kao ni pojmove koje pronalaze web-tražilice
- Preporučljivo je koristiti kombinacije velikih i malih slova, numeričkih i specijalnih znakova (Car, Kralj, 2016).

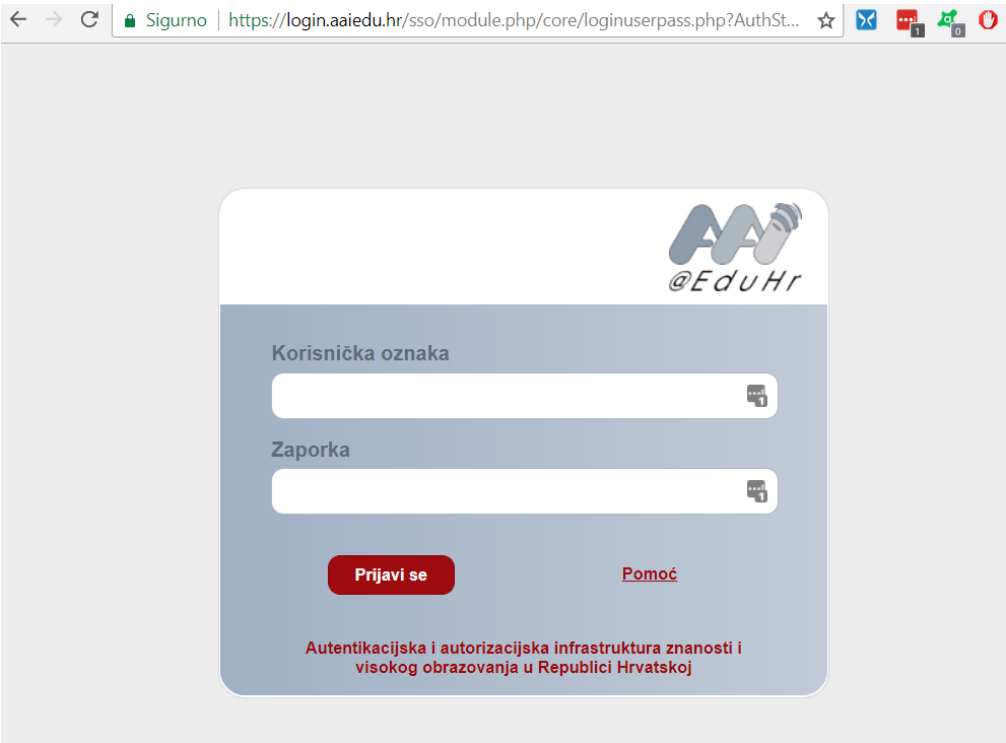
Zaštita privatnog elektroničkog identiteta u sustavu AAI@EduHr od moguće zlouporabe moguća je poštivanjem nekoliko sigurnosnih provjera. Kada se prijavljujete u web-aplikacije, svoje korisničko ime i zaporku upisujte **isključivo** u *login* servis sustavu AAI@EduHr. Za izbjegavanje posjeta lažnoj stranici prije upisa provjerite sljedeće:

- adresa prikazana u adresnoj traci vašega internetskog preglednika treba započeti s https://login.aaiedu.hr/; mora koristiti HTTPS protokol i mora biti potpisana digitalnim certifikatom.



Slika 11. Primjer ispravnog certifikata kojim se dokazuje valjanost web-stranice https://login.aaiedu.hr/

- *login* servis predstavlja se ispravnim certifikatom s potpisom CARNET-a, koji vaš web-preglednik prepoznaje (slika 12)
- vaš web-preglednik ne smije prikazati nikakva sigurnosna upozorenja
- izgled web-stranice na kojoj se prikazuje prijava za sustav AAI@EduHr (slika 13) vrlo je lako krivotvoriti, odnosno uz malo poznavanja razvoja mrežnih stranica i napraviti. Sam izgled ekrana za prijavu prikazan na donjoj slici ništa ne znači i vrlo je vjerojatno krivotvoren **ako nije potvrđen digitalnim certifikatom. Taj digitalni certifikat mora biti izdan isključivo login.aaiedu.hr web-stranici (slika 12). Certifikat mora biti važeći.**



Slika 12. Izgled obrasca za prijavu u sustav AAI@EduHr

Javni digitalni identitet

Pretraživanjem mrežnih stranica, preuzimanjem dokumenata, gledanjem sadržaja na internetu stvaramo svoj **javni digitalni identitet** koji na internetu ostaje trajno. Svaki put kada se na mrežnome portalu prijavimo ili odjavimo, kad nešto objavimo ili preuzmemo s interneta, ostavljamo digitalni trag (Delić, Duvnjak, Ivošević, 2014).

Javni identitet stvaramo pomoću digitalnih tragova koje ostavljamo za sobom pri korištenju internetom. Digitalne tragove kreiramo individualno, izrađujući materijale koje ostavljamo na internetu (npr. članke, blogove, fotografije i sl.). Također, mogu ga stvoriti i druge osobe, i to bez našeg znanja i volje. To su primjerice informacije koje prijatelji objavljuju o vama na društvenim mrežama i mrežnim stranicama.

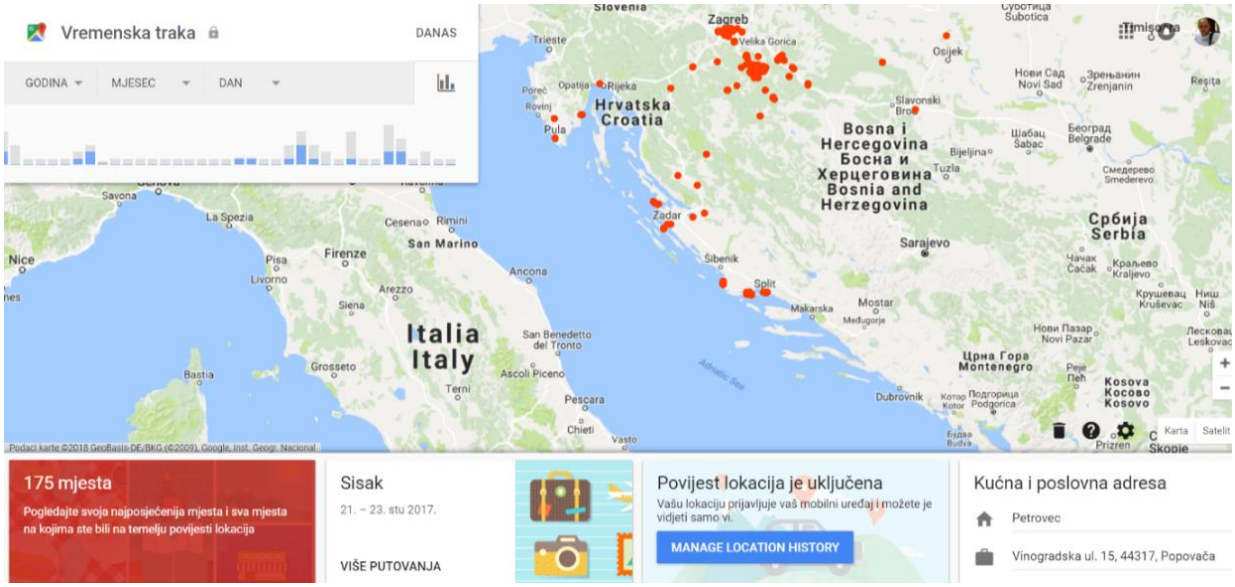
Tragovi koje ostavljamo mogu biti javno dostupni ili vidljivi samo pružateljima usluga. Primjerice, povijest prijavljivanja na određenu uslugu nije javno vidljiva. Ako pak napadač uspije „upasti“ u informacijski sustav pružatelja usluga, podaci koji su inače dostupni samo vlasniku mogu postati dostupni i napadaču.

2.1 Što sve internet zna o meni

Javni identitet i digitalni tragovi koje ostavljamo na internetu. lako su dostupne informacije o bilo kojoj osobi koja se svakodnevno koristi internetskim uslugama. Svi korisnici Googleovih usluga na računalima i mobitelima često pristaju da Google prati sve o njima te da se prikupljenim informacijama koristi za poboljšanje rezultata pretrage interneta. Za provjeru svega što Google prati možete posjetiti adresu https://myactivity.google.com/myactivity.

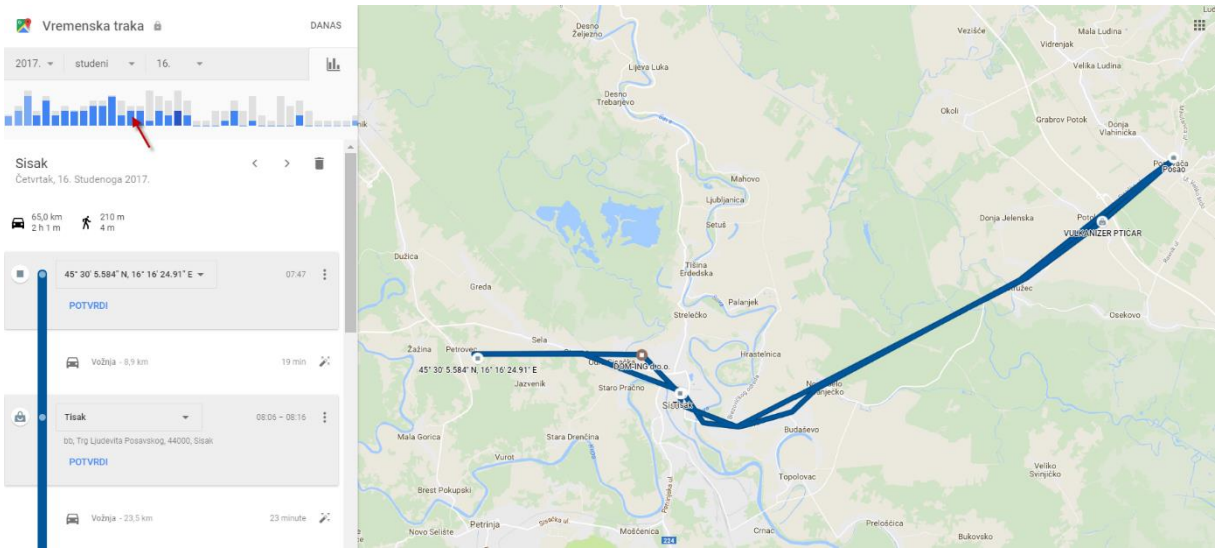
Podaci koje ste unijeli pri otvaranju računa na Googleu te povijest vaše uporabe pretraživača i posjećenih mrežnih stranica Googleu omogućuju stvaranje vašeg profila kojim se koristi za prodavanje usluga oglašivačima. Google omogućuje da posjetom stranici https://adssettings.google.com/authenticated prilagodite teme koje vas zanimaju.

Korisnici pametnih telefona s operacijskim sustavom Android te uključenim GPS sustavom trebaju znati da Google pamti povijest kretanja (lokacije i brzinu kretanja). Te su informacije također dostupne samo vlasniku računa (svakom tko ima vjerodajnice za račun). Google omogućuje da vidimo svoje kretanje na stranici https://www.google.com/maps/timeline.



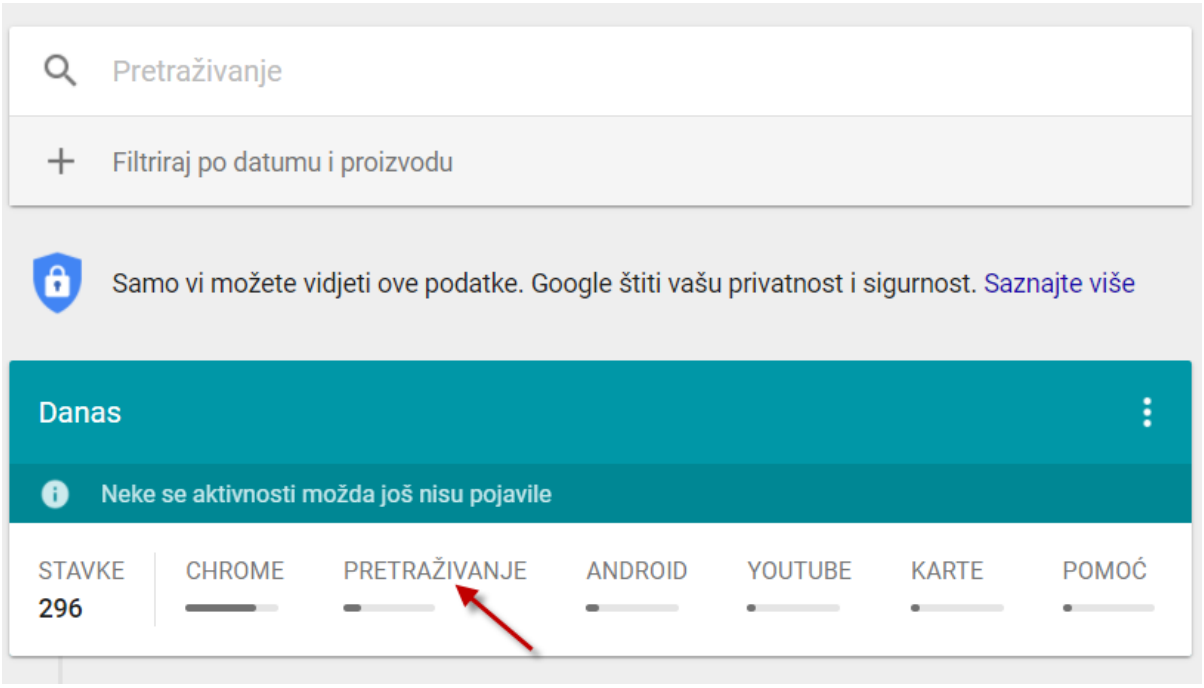
Slika 13. Google vremenska crta

Odabirom pojedinog datuma možete vidjeti detalje kretanja tog dana (vidi sliku 15).



Slika 14. Prikaz kretanja s pomoću Googleove vremenske trake

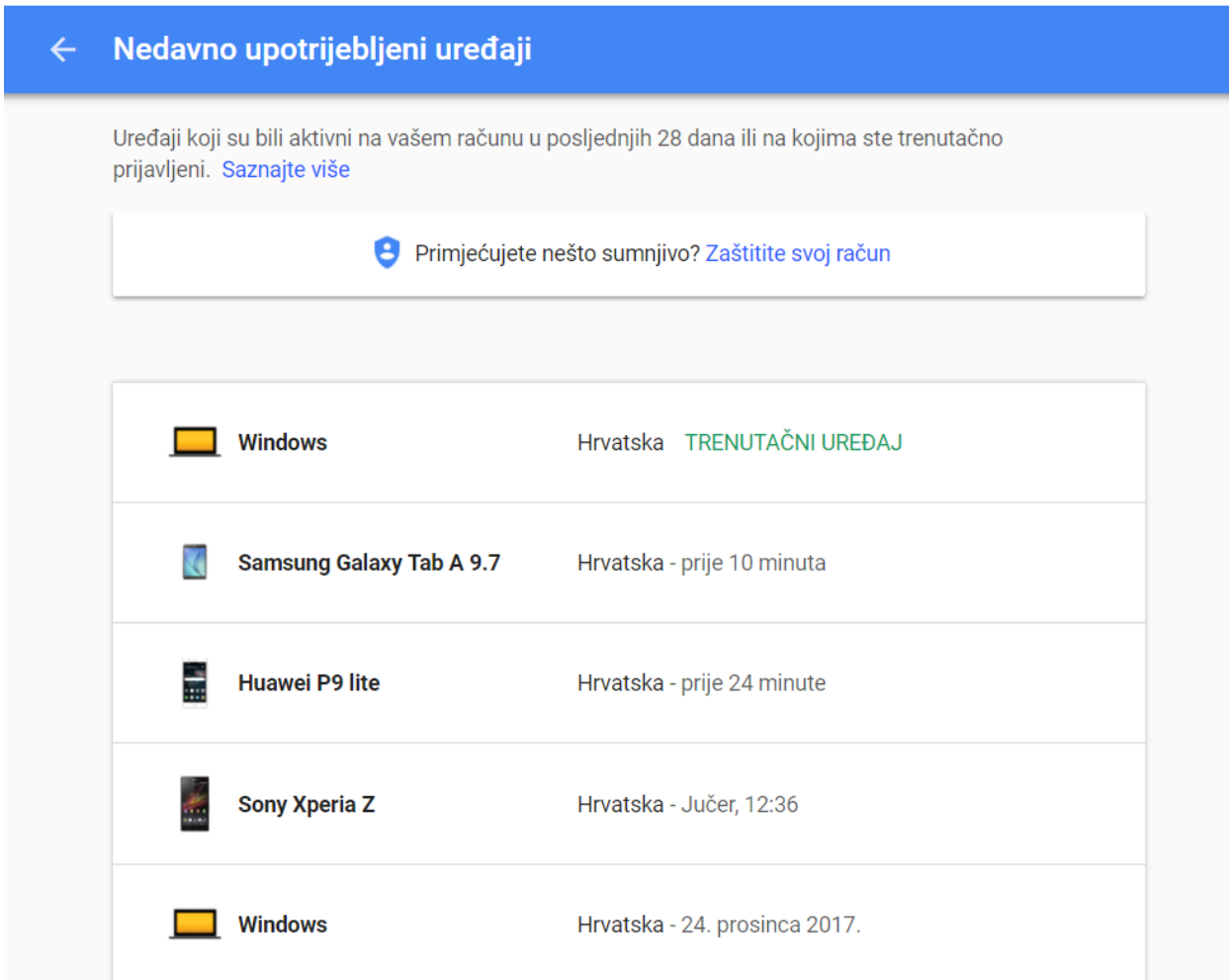
Googleova tražilica pamti svaku vašu pretragu, kao i svaku stranicu koju ste posjetili. Sve pretrage sprema i veže uz vaš korisnički račun te koristi te podatke za određivanje redoslijeda rezultata budućih pretraga. Ako želite provjeriti što ste sve pretraživali na Googleu, posjetite https://myactivity.google.com/myactivity i odaberite Pretraživanje (vidi sliku 16.) Naravno, ovi su rezultati opet vidljivi svima koji imaju vjerodajnice vašega korisničkog računa.



Slika 15. Pregledavanje povijesti pretraživanja Googlea

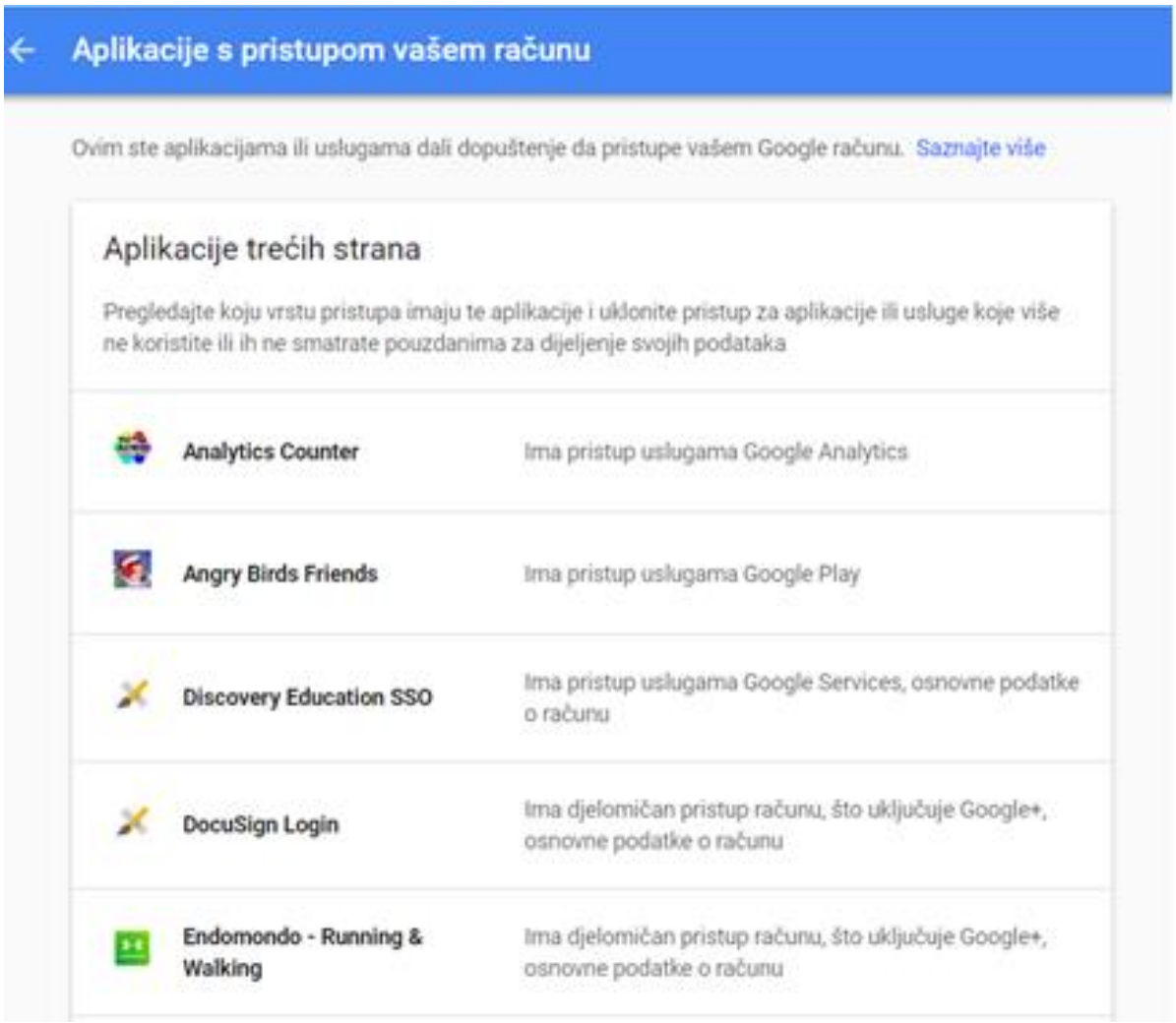
Na ovim stranicama možete pregledati sve što ste tražili u prošlosti i brisati pojedine pretrage. Ukoliko želite spriječiti da Google pamti što ste pretražili i na kojim ste stranicama bili prije upisivanja pojma za pretragu, odjavite se iz vašega Google računa, odaberite drugu tražilicu ili jednostavno pokrenite novi preglednik s postavkama za privatnost.

Google jednako tako zna kojim se sve uređajima koristite kada pristupate svojem računu, a posjetom stranice https://myaccount.google.com/device-activity možete saznati koji su se sve uređaji prijavili na vaš Google račun (slika 17). Ova usluga može biti korisna ukoliko sumnjate na zlouporabu ili provalu u račun.



Slika 16. Popis uređaja kojima pristupate svojem Google računu

Jednako tako, putem poveznice https://myaccount.google.com/permissions možete provjeriti kojim ste sve internetskim aplikacijama i ekstenzijama preglednika dopustili pristup osobnom podacima (vidi sliku 18).



Slika 17. Popis aplikacija i ekstenzija za internetski preglednik kojima ste dopustili pristup informacijama

2.2 Savjeti za zaštitu privatnog i javnog identiteta

Uključivanje anonimnog načina pretraživanja

U anonimnom načinu pretraživanja, kakvo omogućuju moderni internetski preglednici, ne bilježi se ono što ste pretraživali te se ne bilježe podaci koje unosite. Za pokretanje prozora koji omogućuje privatni način pretraživanja koristite se ovim tipkovničkim prečacima:

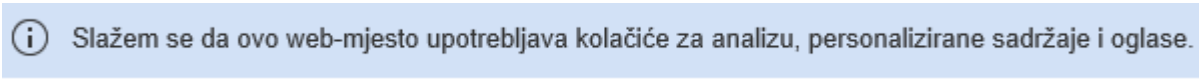
- Google Chrome: Ctrl + Shift + N
- Firefox: Ctrl + Shift + P
- Safari, idite na Safari – Novi privatni prozor.

Za one koji žele znati više

Više o anonimnom načinima pregledavanja i brisanju pretraživanja i aktivnosti u najpoznatijim mrežnim preglednicima možete pronaći ovdje: https://goo.gl/Q2aCkr.

Brisanje kolačića i povijesti pregledavanja

Pružatelji usluga dužni su obavijestiti korisnika ukoliko koriste kolačiće (*Cookies*).



Slika 18. Prikaz obavijesti o upotrebi kolačića

Kolačići (engl. *Cookies*) su datoteke koje se spremaju na računalo dok pregledavamo mrežne stranice, a služe za prepoznavanje korisnika kad se ponovno vrate, kao i u neke druge svrhe. Pružateljima usluga omogućuju da prilagode prikaz sadržaja web-stranice na osnovi prethodnog ponašanja i lokacija na internetskoj stranici na koje su češće kliknuli mišem. Jednako tako, mogu spremiti i vaše vjerodajnice za pristup stranicama, tako da ih kod sljedećeg posjeta ne morate ponovno upisivati. Naravno, to može predstavljati sigurnosni problem, jer ako napadač dođe do vaših kolačića, moći će pristupiti uslugama na koje ste prijavljeni korištenjem kolačića. Ako se koristite mogućnostima anonimnog pregledavanja interneta, ovi podaci ne ostaju na računalu.

Kolačiće možemo obrisati putem opcije mrežnog preglednika. Upute za pojedini preglednik dostupne su ovdje:

- Mozilla Firefox – https://goo.gl/hT7n5r
- Google Chrome – https://goo.gl/H9G6fE
- Microsoft Edge – https://goo.gl/tEq1Tm
- Safari – https://goo.gl/a15oJM.

Isključivanje opcije Moja aktivnost i Google vremenska traka

Google omogućuje isključivanje nekih opcija praćenja. Želimo li onemogućiti praćenje aktivnosti, treba otvoriti poveznicu https://myactivity.google.com/myactivity te odabrati opciju Moj račun te Upravljanje svojim aktivnostima na Googleu.

Zatim, potrebno je otvoriti Kontrole aktivnosti te isključiti opciju Aktivnost na webu i u aplikacijama te Povijest lokacije.

Za isključivanje Google vremenske trake, treba otići na internetsku vezu https://www.google.com/maps/timeline?pb, otvoriti postavke i iz skočnog prozora odabrati postavke vremenske trake koje želimo isključiti.

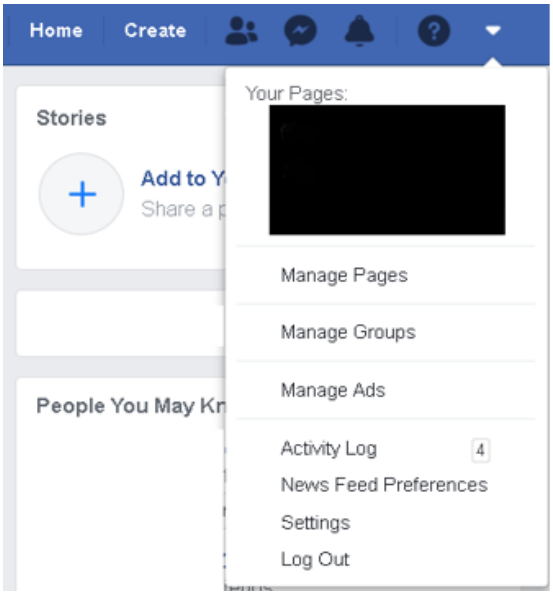
Prilagođavanje postavki privatnosti na društvenim mrežama

I drugi pružatelji usluga imaju postavke privatnosti. Naravno, često pokušavaju zakomplicirati njihovo postavljanje krajnjim korisnicima jer popularnost „leži“ u što manjoj privatnosti. Ako želite provjeriti koji su vaši privatni podaci javno dostupni na Facebooku, možete se poslužiti stranicom https://stalkscan.com/.

Dovoljno je kopirati poveznicu na svoj profil na Facebooku i StalkScan će vam pokazati koliko je vaš profil na Facebooku „privatan“.

Slika 19. Stranica za provjeru javno dostupnih podataka na Facebooku

StalkScan koristi samo javno dostupne informacije, odnosno podatke koji se pojavljuju na Facebookovoj tražilici Graph. Ako nakon ove pretrage smatrate da trebate promijeniti postavke privatnosti, otvorite svoju stranicu na Facebooku i kliknite na Postavke (vidi sliku 20).



Slika 20. Postavke računa na Facebooku

Zatim, odaberite opciju Privatnost i uredite svoje postavke. Također možete urediti i postavke vremenske crte, obavijesti te postavke vezane uz sigurnost i prijavu (vidi sliku 21).

Slika 21. Uređivanje opcija privatnosti na Facebooku

3. poglavlje: **Fizička i elektronička zaštita digitalnog sadržaja**

U ovom poglavlju naučit ćete:

- ☑ mjere informacijske sigurnosti – fizičke i elektroničke
- ☑ što je Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije
- ☑ koji su elementi Pravilnika
- ☑ koje su smjernice Pravilnika o prihvatljivom i odgovornom korištenju informacijsko-komunikacijskim tehnologijama.

Imajući u vidu različite oblike zlonamjernih sadržaja, različite načine na koje zlonamjerne osobe pristupaju kompromitiranju informacijskih sustava, logična je i nužna reakcija svake institucije da sistematizira (i trajno nadograđuje) politike i procedure vezane uz informacijsku sigurnost. U današnje vrijeme, zapravo se radi o nečemu što treba osvijestiti i provesti na razini svake institucije, neovisno o veličini, svrsi, broju zaposlenih, ili broju učenika/studenata. U osnovnom smislu, mjere zaštite informacijske sigurnosti možemo podijeliti na dvije osnovne vrste: fizičke i elektroničke.

Fizička zaštita informacijske opreme i uređaja

Pod pojmom „fizička zaštita“ podrazumijevamo sve fizičke zapreke koje postavljamo pred zlonamjernog korisnika na putu prema krađi informacija na bilo koji od dostupnih načina. Stoga je potrebno:

- informacijsku infrastrukturu institucije izdvojiti u posebne prostorije, klimatizirane, s posebnim besprekidnim napajanjem u slučaju nestanka struje (kako bi se osiguralo dovoljno vremena za mirno gašenje sustava),
- prostorije u kojima se nalazi infrastruktura zaštititi propisanim razinama zaštite od požara, provale, s kvalitetnom bravom te razmisliti o korištenju dodatnih zaštitnih mehanizama (pametne kartice za kontrolu ulaza u prostoriju, ulazak u server sobu korištenjem PIN-a za otvaranje vrata, višestruka autentifikacija i sl.),
- implementirati sustav videonadzora kako bismo imali jednostavan način provjere ulaska u server sobu (uz pripadajuće dokumentiranje politike i procedure korištenja videonadzora, sukladno pravnoj regulativi).

Elektronička zaštita informacijske opreme i uređaja

Pod pojmom „elektronička zaštita“ podrazumijevamo sve potencijalne sigurnosne uređaje i procedure pomoću kojih ćemo onemogućiti zlonamjernog korisnika (ili kod) da napravi probleme u infrastrukturi institucije. Stoga je potrebno:

- implementirati sustav vatrozida na razini institucije, a ukoliko je moguće, kroz dvoslojni pristup (vanjski i unutrašnji vatrozid),
- razmisliti o implementaciji sustava za detekciju upada (*Intrusion Detection System* ili *IDS*),
- razmisliti o implementaciji sustava za zaštitu od upada (*Intrusion Prevention System* ili IPS*),*
- zaštititi sve sadržaje unutar institucije kontrolama pristupa na svim razinama – kroz dozvole na datotečnim sustavima, na raspodijeljenim diskovima, na razini mreže kroz liste kontrole pristupa *(ACL*), logičkim odvajanjem u privatne mreže (*VLAN*) i sl.,
- koristiti pravilo najmanjih privilegija (*least privilege*), tj. dodijeliti svakom korisniku minimalni set prava kako bi mogao obaviti svoj posao, ali ništa više od toga (imajmo na umu da je najveći rizik sigurnosti čovjek,
- implementirati „pomoćne“ alate za detekciju potencijalnih problema u zaštiti digitalnih sadržaja – npr. ukoliko korisnik želi pristupiti nekom sadržaju na raspodijeljenom disku a za to nema prava, možemo otkriti takve događaje korištenjem evidencija za pristup (*audit logging*). Isto tako, ako korisnik želi pristupiti nekom sadržaju kojem bi trebao imati pravo, a nema ga, možemo implementirati sustave za pomoć (npr. *Access Denied Assistance*), kako bi korisnici mogli poslati elektroničku poštu sa zahtjevom za pristup.

Slične mjere možemo primijeniti i na drugim vrstama usluga – internim mrežnim stranicama i servisima, internim aplikacijama i sl. Implementacijom sigurnosnog principa najmanjih privilegija, u svim situacijama kada dodjeljujemo pristup korisnicima, riješit ćemo širu skupinu problema na razini institucije, a ne samo „lokalno“ u specijalnim slučajevima. Korištenje ovog principa obično se temelji na ulogama koje korisnici imaju unutar svojih institucija, što implicira i uređene odnose unutar institucije na razini prava i obaveza svakog pojedinog zaposlenika. Tako ćemo moći sistematski regulirati pristup resursima tvrtke, s manje straha da će doći do sigurnosnih problema.

Do sada smo, kroz mjere informacijske sigurnosti, razmatrali pristup koji bi trebalo primjenjivati (sa stajališta tvrtke), prema krajnjim korisnicima. Međutim, razmatrali smo to parcijalno, kroz prijedloge različitih mjera koje možemo pojedinačno provesti. Ali, obično se ovakve mjere i procedure gledaju u „širem smislu“, kao dio šire strategije korištenja informacijske infrastrukture institucije, zbog čega je potrebno napraviti dodatnu dokumentaciju. Jedan od osnovnih dokumenata u tom smislu je i Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije.

Tajnost i klasifikacija podataka

Tajnost podataka jedna je od osnova usluge koju institucije nude svojim učenicima i studentima – ne objavljujemo javno ocjene na oglasnim pločama, ne dijelimo podatke o zdravstvenoj situaciji učenika (osim u strogo dogovorenim procedurama unutar odjela institucije) i sl. Isto tako, nužno je osigurati tajnost podataka i u našim informacijskim sustavima – inicijalno kroz dozvole na razini datotečnih sustava i na razini raspodijeljenih direktorija.

Iduća razina sigurnosti koju možemo implementirati na proceduralnoj i tehničkoj razini su klasifikacije podataka. Vjerojatno ste nekada vidjeli dokumente koji na sebi imaju oznaku „Tajno“, „Povjerljivo“ i slično. Oznake tajnosti mogu varirati od sustava do sustava i biti propisane na razini države (npr. za sustav državne uprave) ili na razini tvrtke (s obzirom na poslovne procese tvrtke). Upravo je to ideja klasifikacije podataka – da se različito osjetljivi dokumenti označe različitim oznakama tajnosti koje se onda na proceduralnoj razini tretiraju kroz različite nivoe dozvola na razini institucije. Primjera radi, ako se politikom klasifikacija uvede procedura koja zabranjuje da zaposlenici odjela marketinga imaju pristup dokumentima s klasifikacijom „Povjerljivo“, onda treba napraviti poslovni proces koji će to podržati u praksi. Iste se takve procedure mogu napraviti i na razini datotečnog poslužitelja – označiti dokumente različitim oznakama tajnosti kako bi se kroz te oznake odmah upozorilo na nivo tajnosti.

Nužno je spomenuti da se korištenje klasifikacija u sustavu državne uprave obično razlikuje od korištenja klasifikacija u privatnim tvrtkama. U sustavu državne uprave redovito se radi o podacima iz sustava obrane, policije i tajnih službi, koji su sami po sebi osjetljivi na razini cijele države. Kod privatnih tvrtki djelomično se radi o klasificiranju podataka radi sprječavanja curenja informacija prema osobama u tvrtki koje ne bi trebale imati pristup podacima, ali češće je to dio cjelokupnog procesa zaštite od curenja podataka prema konkurentskim tvrtkama.

3.1 Što je Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije

Obzirom na sve veću informatizaciju obrazovnih ustanova te prijetnje i rizike kojima su svi korisnici IKT-a svakodnevno izloženi, nužno je posvetiti veliku pozornost sigurnoj i odgovornoj primjeni IKT-a u školama te definiranju načina ponašanja, pravila i procedura djelovanja pri upotrebi IKT-a.

Upravo zato, CARNET je izradio dokument **Prijedlog strukture Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske** tehnologije s ciljem da škole, slijedeći upute, izrade vlastiti Pravilnik koji će poštovati sve zadane elemente, ali sadržavati i pravila i procedure za sve ostale usluge i/ili teme kojima se određena škola bavi, vezane za IKT, a da u ovom dokumentu nisu navedene.

Osnovni elementi Pravilnika

Osnovni elementi koje bi Pravilnik o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije trebao sadržavati (CARNET, 2017) su:

- **Uvod** – potrebno je jasno navesti koja je svrha Pravilnika, na koga se sve i na koji način odnosi.
- **Osnovne sigurnosne odredbe –** potrebno je naglasiti važnost očuvanja sigurnosti informacija vezanih uz svaki aspekt djelovanja škole i njezinih djelatnika i učenika, ali i očuvanja IKT infrastrukture u školi te utjecaja ljudskog čimbenika.
- **Školska IKT oprema i održavanje –** potrebno je specificirati školsku IKT opremu i način njezina održavanja.
- **Reguliranje pristupa IKT opremi – potrebno je** regulirati i precizirati tko ima pristup pojedinim IKT resursima.
- **Sigurnost korisnika** – nužno je definirati sve mjere sigurnosti vezane uz korisnika i utvrditi poželjna pravila ponašanja.
- **Prihvatljivo i odgovorno korištenje informacijsko-komunikacijskim tehnologijama** – potrebno je definirati pravila i upute za prihvatljivo korištenje internetom i društvenim mrežama. Također, potrebno je definirati zaštitu autorskih prava korisnika te izraditi upute o dijeljenju podataka, kao i definirati što se smatra internetskim nasiljem i kakve su sankcije za one koji ga primjenjuju.

3.1.1 Prihvatljivo i odgovorno korištenje informacijsko-komunikacijskim tehnologijama

Dio Pravilnika koji se odnosi na **prihvatljivo i odgovorno korištenje informacijsko-komunikacijskim tehnologijama** bit će podijeljen na više područja.

<u>Ponašanje na internetu</u>

U sklopu ovog dijela Pravilnika „škola mora definirati postojanje općeprihvaćenog skupa pravila ponašanja na internetu – 'Netiquette' te načine upoznavanja svih

korisnika s tim pravilima, npr. da će ona biti izvješena u informatičkim učionicama i nekim drugim mjestima. Isto tako, važno je napomenuti kako je svaki pojedinac odgovoran za svoje ponašanje u virtualnom svijetu te da se prema drugim korisnicima mora ponašati pristojno, ne vrijeđati ih niti objavljivati neprimjerene sadržaje“ (CARNET, 2017).

Dakle, u ovom je dijelu Pravilnika vrlo važno izraditi konkretna i jasna pravila ponašanja vezana uz sigurnost na internetu, ali i svojevrsni internetski bonton, odnosno pravila lijepog ponašanja na internetu. Primjere tih pravila moguće je pronaći upravo u CARNET-ovu dokumentu Prijedlog strukture Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije.

Autorsko pravo

U ovom dijela Pravilnika vrlo je važno korisnike uputiti na definiciju autorskih prava koja se tiču digitalnih sadržaja, računalnih programa i IKT opreme te na koji način trebaju štititi i poštovati svoja i tuđa autorska prava pri upotrebi i/ili izradi materijala te pri korištenju računalnih programa i opreme.

„Ovdje je potrebno istaknuti da se korisnike potiče da potpisuju materijale koje su sami izradili koristeći neku licencu poput Creative Commons, ali i da poštuju tuđe radove. Nipošto ne smiju tuđe radove predstavljati kao svoje, preuzimati zasluge za tuđe radove, niti nedopušteno preuzimati tuđe radove s interneta. Korištenje tuđih materijala s interneta mora biti citirano, obvezno navodeći autora korištenih materijala te izvor informacije (poveznica i datum preuzimanja)“ (CARNET, 2017).

U sklopu pilot projekta e-Škole razvijen je priručnik za webinar o intelektualnom vlasništvu, a dostupan je na poveznici (https://www.e-skole.hr/wp-content/uploads/2016/12/Priru%C4%8Dnik_Intelektualno-vlasni%C5%A1tvo.pdf).

Dijeljenje datoteka

Ovdje treba jasno definirati pod kojim uvjetima i tko može dijeliti digitalne datoteke te što smatramo nelegalnim dijeljenjem datoteka.

Internetsko nasilje

U ovom je dijelu Pravilnika potrebno definirati što se smatra nasilničkim ponašanjem na internetu i koje su sankcije koje će se poduzeti ukoliko se utvrdi da je netko u ustanovi provodio takve nedopuštene aktivnosti. Uputno je da se jasne poruke o takvom ponašanju šalju na predmetima tijekom kojih se koristi tehnologija ili na Satu razrednika te da pravila o prihvatljivom ponašanju i korištenju tehnologijom budu vidljiva i u prostorijama škole (CARNET, 2017).

Korištenje mobilnih telefona

Potrebno je utvrditi kada je i pod kojim uvjetima moguće koristiti mobilne telefone na nastavi i u školi općenito. Važno je napomenuti da većina učenika ima mobilne telefone s pristupom internetu pa je nužno ovaj odjeljak povezati s ranije definiranim pravilima ponašanja na internetu (Sigurnost i pravila lijepog ponašanja) (CARNET, 2017).

Savjet

Svakako detaljno proučite dokument: Prijedlog strukture Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije u kojem ćete pronaći detaljnije upute o izradi Pravilnika i dodatne preporuke za što bolje definiranje svakog dijela.

U nastavničkoj se praksi mogu pojaviti sljedeći problemi:

- komuniciranje na nastavi i/ili ispitu putem mobilnog telefona,
- upotreba mobilnog telefona za nesamostalno rješavanje zadataka,
- audio-, video- i fotosnimanje nastave,
- korištenje mobilnog telefona u svrhu omogućavanja praćenja nastave osobama koje nisu prisutne,
- zahtjevi roditelja za komuniciranjem s učenicima u vrijeme nastave,
- zahtjevi da preko mobilnog telefona prate i kontroliraju nastavu,
- neispravnost mobilnog uređaja na nastavi kada se očekuje suprotno itd.

Za one koji žele znati više

Pogledajte neke primjere Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije:

Osnovna škola Mijat Stojanović Babina Greda https://goo.gl/hQrVe4

XV. Gimnazija, Zagreb https://goo.gl/xvNNb6.

4. poglavlje: **Zaštita privatnosti i zakonski okviri zaštite privatnosti**

U ovom poglavlju naučit ćete:

- ☑ što su privatnost i osobni podaci
- ☑ kako zaštititi privatnost
- ☑ kako zaštititi privatnost djece
- ☑ koji su zakonski okviri zaštite privatnosti
- ☑ što je Opća Uredba o zaštiti osobnih podataka
- ☑ što je Izjava o privatnosti.

Privatnost je osnovno ljudsko pravo, a „pravo privatnosti je jedna od nosivih vrednota zapadne pravne kulture. Zasnovana je, s jedne strane, na uvjerenju da svako ljudsko biće ima vrijednost po sebi, a s druge na iskonskoj čovjekovoj potrebi za postojanjem određenog zaštićenog prostora iz kojega bi svatko drugi bio isključen psihološki i materijalno“ (Boban, 2012:581).

Prema definiciji koju je propisao stari Zakon o zaštiti osobnih podataka („Narodne novine“ broj 106/12 – pročišćeni tekst) „osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati; osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.“ Ovakva je definicija prenesena i u Zakon o provedbi Opće uredbe o zaštiti podataka, koja je stupila na snagu 25. svibnja 2018., nakon čega je Zakon o zaštiti osobnih podataka stavljen izvan snage.

Osobni su podaci, primjerice:

- adresa fizičke osobe,
- broj telefona/mobitela,
- e-adresa,
- osobna fotografija,
- identifikacijski broj,
- biometrijski podaci (otisak prsta, snimak šarenice oka),
- podaci o obrazovanju i stručnoj spremi,
- podaci o osobnom dohotku,
- podaci o kreditnom zaduženju,
- podaci o računima u banci.

Kako zaštititi privatnost na internetu

Kako biste zaštitili privatnost na internetu (prema AZOP, 2011), bitno je pridržavati se nekoliko osnovnih pravila ponašanja. Možemo ih podijeliti u dvije kategorije: one koje govore o pravima te zašto treba štititi te podatke i one koje govore kako to najbolje učiniti.

Prava pri zaštiti osobnih podataka te zašto podatke treba štititi:

- zaštitom svojih osobnih podataka štitimo sebe od izloženosti, a time i od mogućih iskorištavanja,
- osobni podaci na internetu smiju se prikupljati i obrađivati samo ukoliko smo za to dali pristanak,
- tuđe osobne podatke smijemo dijeliti samo ako smo za njih dobili pristanak.

Načini kako zaštititi zaštite osobnih podataka:

- nikada ne koristiti osobne podatke i poznate riječi u zaporkama (poglavlje 2.1.1 Privatni digitalni identitet),
- uvijek upotrebljavati barem jednu brojku i barem jedno veliko slovo pri kreiranju zaporki te barem jedan kontrolni znak (upitnik, uskličnik i sl.),
- ne koristiti se istim zaporkama na različitim internetskim stranicama i servisima,

- pri registraciji na nekoj mrežnoj stranici potrebno je popuniti samo ona polja koja su nužna; ako se postupak registracije ne može nastaviti bez podataka koje ne smatramo nužnima, treba procijeniti opravdanost takve radnje kao i sigurnost i vjerodostojnost te stranice,
- e-poštom šaljemo osobne podatke samo prema provjerenim adresama, a pri *online* plaćanju koristimo se uslugama provjerenih partnera (poput *PayPal*-a),
- nužno je pročitati i opće uvjete te sve „ono napisano sitnim slovima“; većina takvih uvjeta ne mora nužno biti razumljiva svima pa se za pomoć treba obratiti stručnim osobama,
- kolačići se mogu obrisati putem internetskog preglednika pa ih je potrebno redovito brisati,
- nužno je koristiti antivirusne programe,
- nikada ne upotrebljavati zaporke kraće od šest znakova,
- s vremena na vrijeme pitati veće tvrtke koje imaju naše podatke (npr. T-Com i sl.) koje podatke o nama imaju i napraviti modifikaciju podataka ukoliko su netočni (kada nam je u interesu da podaci budu ispravni) ili tražiti njihovo brisanje (ako ne postoji razlog zašto bi tvrtke imale naše podatke, npr. nakon što smo prekinuli ugovor za isporuku usluga i podmirili sve račune).

Zaštita privatnosti djece u digitalnom okruženju

Zaštita privatnosti djece u digitalnom okruženju posebno je osjetljiva tema, obzirom na načine na koje djeca danas dolaze do informacija (većinom koristeći internet), kao i činjenicu da djeca danas već najranije dobi koriste tehnologiju za različite svrhe – od slušanja glazbe i gledanja filmova, preko razgovora korištenjem socijalnih mreža i različitih sustava za razmjenu poruka, do igranja igrica na računalu, tabletu ili mobilnom telefonu. Nerijetke su situacije u kojima dijete, bez nadzora roditelja, koristi npr. tablet za pristup nekoj igrici koju koristi i veliki broj druge djece (npr. Minecraft), gdje je mogućnost izvlačenja podataka od djece puno veća nego u slučaju ukoliko dijete sjedi pored nas a netko pokušava s njim razgovarati. Privatnost djece je posebna kategorija kojom se treba svakodnevno baviti i to kroz edukacije i primjere iz prakse/života. Primjera radi, možemo pokušati sljedeće:

- učiti djecu da nikada za vrijeme igranja na internetu ne odaju podatke o sebi – ime, prezime, adresu, i slične podatke,
- učiti djecu da, ukoliko im netko postavlja čudna pitanja u prozoru za razgovor u nekoj igrici, nam to odmah kažu,
- odrediti vrijeme unutar kojeg djeca mogu konzumirati različite sadržaje kroz sigurnosne politike – s vremena na vrijeme, ako za to postoji mogućnost, isključiti pristup internetu i smisliti neki drugi edukativni sadržaj za koji pristup internetu nije potreban,
- kroz korištenje tehničkih i sigurnosnih mjera suziti količinu mrežnih stranica na koje se može pristupiti tako da djeca imaju manju priliku doći u kontakt sa sumnjivim sadržajima – za ovakve politike nužno su potrebni npr. vatrozidi zadnjih nekoliko generacija.

Zakonski okvir zaštite privatnosti

Prema starom Zakonu o zaštiti osobnih podataka (Narodne Novine, 106/12) „zaštita osobnih podataka u RH je ustavna kategorija te je osigurana svakoj fizičkoj osobi u RH bez obzira na državljanstvo i prebivalište, neovisno o rasi, boji kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili osobinama“.

Dodatno, privatnost i njezina zaštita definirana je Ustavom Republike Hrvatske (Narodne Novine 85/2010) u članku 37. koji ističe da se „svakom jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika, osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom.“

Nadzor nad prikupljanjem, obradom i korištenjem osobnih podataka u Republici Hrvatskoj od 25. svibnja 2018. uređuje se Općom uredbom o zaštiti podataka (Uredba 2016/679 Europskog parlamenta i Vijeća) i Zakonom o provedbi Opće uredbe o zaštiti podataka (Narodne Novine 42/2018).

Što je Opća uredba o zaštiti osobnih podataka

Opća uredba o zaštiti osobnih podataka (EU 2016/679) je pokušaj da se pitanje zaštite osobnih podataka konačno pokuša sustavno staviti u kontekst vremena u kojem živimo – vremena u kojem su osobni podaci svugdje oko nas. Mi najčešće ne znamo kako se koriste i imamo relativno malo prava da s njima na ikoji način raspolažemo. Primjera radi: kako da točno znamo što servis, kao što je Facebook, radi s našim podacima(kao korisnika9? Dijeli li te podatke s nekim trećim stranama? Ili, općenito, postoje li situacije u kojima se takvi podaci dijele između različitih tvrtki, pa čak i za ostvarenje materijalne koristi?

Iako su naša zakonska rješenja koja reguliraju tretman osobnih podataka mijenjana kroz vrijeme (između 2003. i 2012. godine), na razini EU je osviješteno kako je potrebno napraviti zajednički okvir koji bi se u praksi primjenjivao kao ujednačeni „standard“ za rad s osobnim podacima građana EU. To je i jedan od razloga zašto je na razini EU 2016. izglasana Opća uredba o zaštiti osobnih podataka. Izglasana je kako bismo kao privatne osobe dobili veću količinu prava i informacija o onome što se s našim podacima radi. Opća uredba također sadrži i regulativu o izvozu i prijenosu podataka izvan EU, što je već dulje vrijeme jedna od spornih točaka u odnosima između privatnih osoba i različitih korporacija diljem svijeta.

Zbog činjenice da se ne radi o direktivi, nego o uredbi, na razini zakonodavstva svake pojedine države nije potrebno donositi dodatne zakonske ili druge akte kako bi se Uredba primijenila, već se, neovisno o nacionalnom zakonodavstvu, primjena odnosi na sve pravne subjekte, u svim slučajevima kada su u pitanju osobni podaci građana EU/EEA.

Implementacija Opće uredbe o zaštiti osobnih podataka prodire duboko u poslovni i organizacijski spektar svake institucije, budući se provodi prema o metodologiji vrlo sličnoj implementaciji ISO 27001 certifikata s naglaskom na osobne podatke. Osim toga, duboko zahvaća i u sigurnosne i informacijske sustave, i upravo zato implementaciji treba pristupiti sustavno. Parcijalne implementacije ne donose punu sukladnost, mogu izazvati probleme i kazne, što posljedično može završiti i gubitkom ugleda institucije.

Izjava o privatnosti

Tijekom našeg pregledavanja mrežnih stranica na internetu, svakodnevno se i stalno prikupljaju naši osobni podaci. Svaka mrežna stranica, odnosno tvrtka ili organizacija koja iza nje stoji, na taj način stvara bazu podataka o svojim korisnicima. Vrlo je važno znati koji se naši osobni podaci prikupljaju i na koji se način upotrebljavaju, a te bi se informacije morale naći na svakoj mrežnoj stranici koja na bilo koji način prikuplja osobne podatke.

Upravo dokument koji se zove **Izjava o privatnosti** opisuje načine na koje se „rukuje“ s našim osobnim podacima.

Izjava o privatnosti dokument je u kojemu su jednostavnim jezikom objašnjena pravila: koje podatke određena mrežna stranica prikuplja, kako ih upotrebljava i dijeli.

Stoga bi prije ostavljanja osobnih podataka na nekoj mrežnoj stranici, obvezno trebalo pročitati Izjavu o privatnosti koja se još zove i Politika privatnosti.

Izjava o privatnosti trebala bi sadržavati ove elemente:

- tip osobnih podatka koji se prikupljaju,
- razlog zbog kojeg se navedeni podaci prikupljaju,
- kako će se prikupljeni podaci upotrebljavati,
- tko će se sve koristiti prikupljenim podacima,
- kako se prikupljeni podaci štite i pohranjuju,
- kako se postupa s osobnim podacima djece i mladih,
- na koji način korisnik može pristupiti prikupljenim podacima,
- tko je kontaktna osoba koja je zaduženja za pojašnjenja Izjave o privatnosti,
- vrijeme zadržavanja podataka (CARNET, 2005).

Za one koji žele znati više

Pogledajte nekoliko primjera Izjave privatnosti:

https://privacy.microsoft.com/hr-hr/privacystatement

https://erasmusplusols.eu/hr/izjava-o-privatnosti/

https://www.facebook.com/policy.php

https://www.etwinning.net/hr/pub/privacy_policy.htm.

Vježba

Otvorite omiljeni internetski portal ili društvenu mrežu. Pronađite i pročitajte Izjavu privatnosti.

Zaključak

Zaštita digitalnog sadržaja i osobnih podataka tema je o kojoj treba neprestano razmišljati pri uporabi računala, bez obzira je li riječ o osobnom ili poslovnom kontekstu. Ako nećemo razmišljati o zaštiti i poduzimati odgovarajuće korake kako bismo i mi i sustav bili sigurni, najvjerojatnije ćemo postati žrtva nekoga zlonamjernog programa ili zlonamjerne osobe, odnosno hakera. Na žalost, većina korisnika danas ne razmišlja o zaštiti ili se, oni koji razmišljaju o tome, povode stajalištem: „Siguran sam – imam antivirusni program“. Je li dovoljno instalirati antivirusni program i konfigurirati vatrozid i smatrati da smo sigurni ? Odgovor je vrlo jednoznačan: nije.

Govoreći danas o zaštiti računala, informacijskih sustava te digitalnog sadržaja, vrlo je bitno imati model sveobuhvatne zaštite. Sveobuhvatna zaštita jest model pristupa zaštiti informacijskim sustavima sa što je moguće više strana kako bi ga se učinilo otpornijim na razne napade s kojima se susrećemo.

Model sveobuhvatne zaštite temelji se na pet stupova koji čine koherentnu cjelinu. To su:

- sigurnost računala (uz pomoć redovitih nadogradnji, antivirusnih programa i vatrozida)
- sigurnost podataka (šifriranje podataka i korištenje šifriranih veza za razmjenu podataka)
- sigurnost mreže (pri čemu najveću ulogu imaju naši mrežni administratori, a nama preostaje izbjegavanje spajanja na tzv. nezaštićene mreže)
- fizička sigurnost (pri čemu treba paziti da računalo ne ostavimo dostupno stranim ljudima, imajući na umu prvo pravilo sigurnosti: Ako nekome dopustite fizički pristup računalu, to više nije vaše računalo)
- politike i procedure te osviještenost korisnika.

U priručniku su se nastojali obuhvatiti svi osnovni aspekti zaštite digitalnog sadržaja i pojedinca u digitalnom okruženju. S napretkom tehnologija većina se prijetnji može spriječiti, no uz nužnu pretpostavku: potrebno je podizanje svijesti korisnika o potencijalnim opasnostima.

Popis literature

AZOP – Agencija za zaštitu osobnih podatka (2016). *Krađa identiteta – brošura.* Dostupno na http://azop.hr/images/dokumenti/217/kradja_identiteta.pdf, pristupljeno 23. 12. 2017.

AZOP – Agencija za zaštitu osobnih podatka (2011). *Sigurno surfanje- zaštita osobnih podataka na internetu.* Dostupno na http://azop.hr/images/dokumenti/217/sigurno_surfanje.pdf, pristupljeno 2. 1. 2018.

Boban, M. (2012) *Pravo na privatnosti i pravo na pristup informacijama u suvremenom informacijskom svijetu*, Zbornik radova Pravnog fakulteta u Splitu, 49 (3), str. 575598.

Car, D., Bobovec, D. (2015) *IT sigurnost*, Zagreb: Algebra d.o.o.

Car, D., Kralj, L. (2016) *Office365*, Zagreb: Hrvatska akademska i istraživačka mreža – CARNET.

CARNET (2005) *Privatnost s P3P tehnologijom*. Dostupno na https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2005-01-105.pdf, pristupljeno 27. 6. 2018.

CARNET (2008) *Elektronički identitet*. Dostupno na https://www.CARNet.hr/elektronicki_identitet, pristupljeno 2. 1. 2018.

CARNET (2013) Brošura *Opasnosti Facebooka*. Dostupna na http://www.cert.hr/sites/default/files/Opasnosti%20Facebooka.pdf, pristupljeno 5. 1. 2018.

CARNET (2017) *Prijedlog strukture Pravilnika o sigurnoj i odgovornoj upotrebi informacijsko-komunikacijske tehnologije*. Dostupno na https://goo.gl/TN56qZ, pristupljeno 5. 1. 2018.

Delić, Z. i sur. (2014) *Sigurnost djece na internetu. Modul 1- priručnik za roditelje 1. i 2. razreda osnovne škole.* Dostupno na http://www.petzanet.hr/Portals/0/Users/009/09/9/Roditelji_Modul_1.pdf, pristupljeno 3. 2. 2018.

Đurđević i sur. (2014) *Sigurnost djece na internetu. Modul 3. Udžbenik za učenike 5. i 6. razreda osnovne škole*. Dostupno na http://www.petzanet.hr/Portals/0/Kurikulum/Udzbenik/Modul3/Modul_3.pdf, pristupljeno 2. 1. 2018.

HAKOM (2016). Dostupan na http://privatnost.hakom.hr/, pristupljeno 5. 1. 2018.

Nacionalni CERT (2016a) Dostupno na http://www.cert.hr/, pristupljeno 5. 1. 2018.

Nacionalni CERT (2016b) *Sigurnije na internetu*. Dostupno na http://cert.hr/dokumenti/sigurnije_na_internetu, pristupljeno 5. 1. 2018.

Narodne novine (2010) *Ustav Republike Hrvatske* (Narodne Novine 85/2010). Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2010_07_85_2422.html, pristupljeno 15. 1. 2018.

Narodne novine (2012) *Zakon o zaštiti osobnih podataka* (Narodne Novine 106/12). Dostupno na https://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html, pristupljeno 14. 1. 2018.

Sveučilišni računski centar (Srce) (2017) Dostupno na http://www.srce.unizg.hr/, pristupljeno 4. 1. 2018.

Impressum

Nakladnik: Hrvatska akademska i istraživačka mreža – CARNET

Projekt: „e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot-projekt)“

Urednica: Ana Belin Šimić

Autori: Dario Car, prof.; Vedran Dakić, pred.

Lektorica: Valentina Horvatić, prof.

Recenzent: dr. sc. Predrag Pale, doc.

Priprema, prijelom: Algebra

Zagreb, srpanj 2018.

Kontakt

Hrvatska akademska i istraživačka mreža – CARNET

Josipa Marohnića 5, 10000 Zagreb

tel.: +385 1 6661 555

www.carnet.hr

Više informacija o EU fondovima možete pronaći na web stranicama Ministarstva regionalnoga razvoja i fondova Europske unije: www.strukturnifondovi.hr.

Ovaj priručnik izrađen je u s ciljem podizanja digitalne kompetencije korisnika u sklopu projekta e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt), koji sufinancira Europska unija iz europskih strukturnih i investicijskih fondova. Nositelj projekta je Hrvatska akademska i istraživačka mreža – CARNET.