

Zaštita digitalnog sadržaja i pojedinca u digitalnom okruženju



CARNET

Cilj webinara

- Steći **znanja i vještine** te primjenjivati **dobre prakse** vezane uz:
 - **identificiranje** mogućih **rizika i prijetnji**
 - koje su moguće kod pristupa i dijeljenja digitalnog sadržaja te sudjelovanja u digitalnom okruženju
- **Poznavanje i osmišljavanje** sigurnosnih i zaštitnih **mjera**
 - npr. fizička i elektronička zaštita
- **Prosudživanje načina zaštite** osobnih podataka i privatnosti u digitalnom okruženju

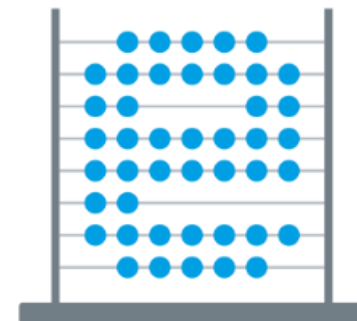
Ishodi učenja

- Identificirati rizike i prijetnje u digitalnom okruženju
- Identificirati postupke zaštite sebe i drugih od mogućnosti opasnosti prilikom dijeljenja podataka u online okruženju
- Identificirati načine zaštite uređaja i digitalnog sadržaja
- Identificirati jednostavne sigurnosne i zaštitne mjere u digitalnom okruženju

Srednja razina digitalnih kompetencija iz područja Digitalni izvori i materijali

Sadržaj webinara

trajanje	sadržaj, aktivnosti
5 min	Uvod u webinar
30 min	Rizici prijetnje u digitalnom okruženju
20 min	Digitalni identitet
5 min	Fizička i elektronička zaštita digitalnog sadržaja
20 min	Zaštita privatnosti i zakonski okviri zaštite privatnosti
10 min	Završna rasprava

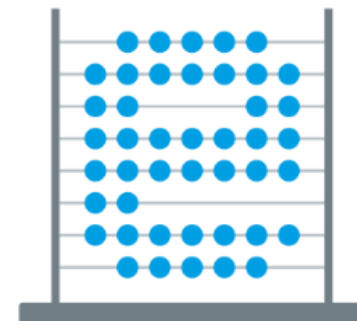


e-Škole

Uvod

Za početak – kratka anketa

Molim da se uključite u anketu i na sljedeće izjave odgovorite da ili ne.



e-Škole

Rizici i prijetnje u digitalnom okruženju

Rizici i prijetnje

- kroz presjek skupova prijetnje, sredstva i ranjivosti definiramo rizik
- rizik, prijetnje i ranjivosti pokušavamo izbjeći ili spriječiti
- ciljane i indirektne prijetnje



Odnos prijetnje, sredstva, ranjivosti i rizika, izvor [ThreatSketch](#)

Ciljane i indirektne prijetnje

- Indirektne prijetnje:
 - automatiziranje, usmjerene na veliki broj ljudi
 - primjer: spam poruke.
- Ciljane prijetnje:
 - B. Schneier: „Samo amateri napadaju računala, a profesionalci ljude.“.

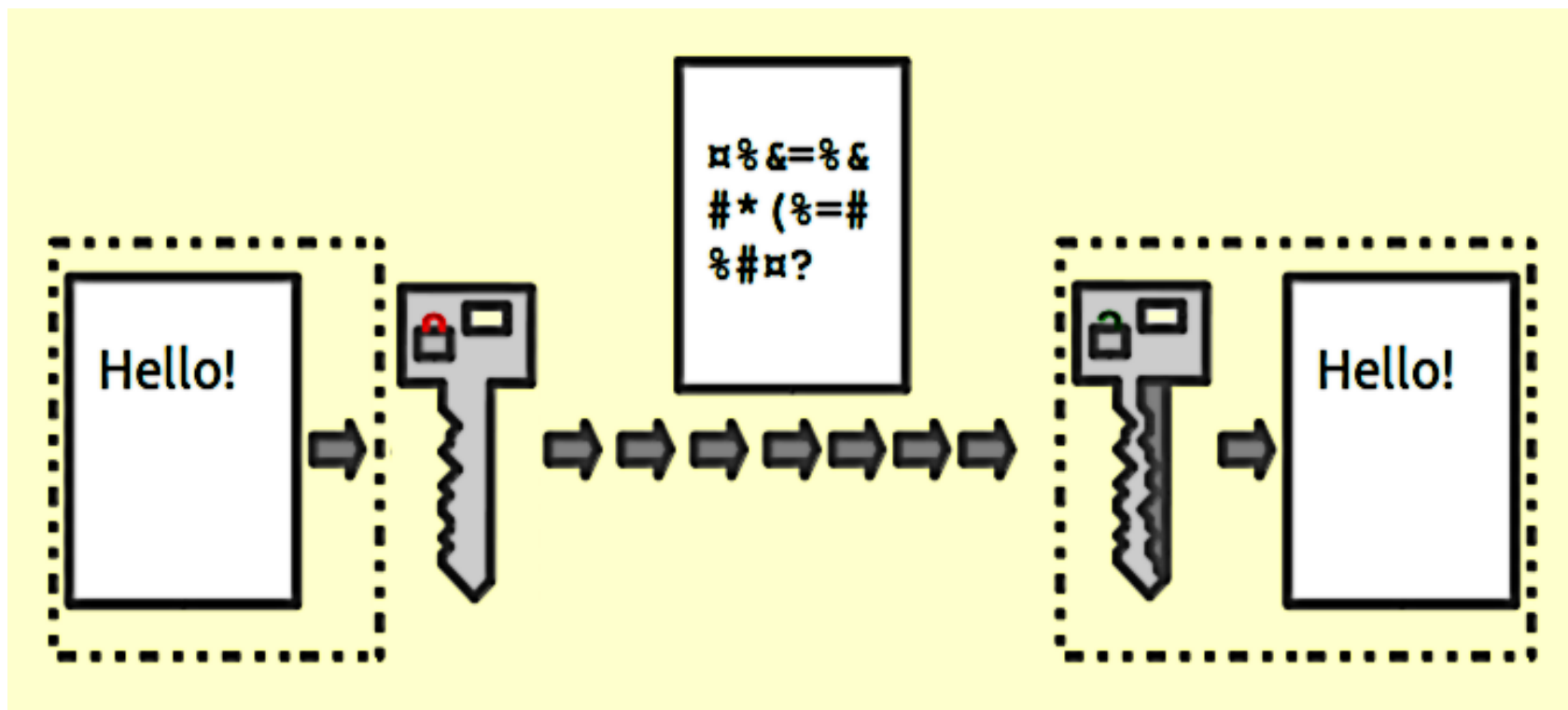


[Ta fotografija](#) korisnika Nepoznat autor: licenca CC BY-SA

Osnove internet sigurnosti

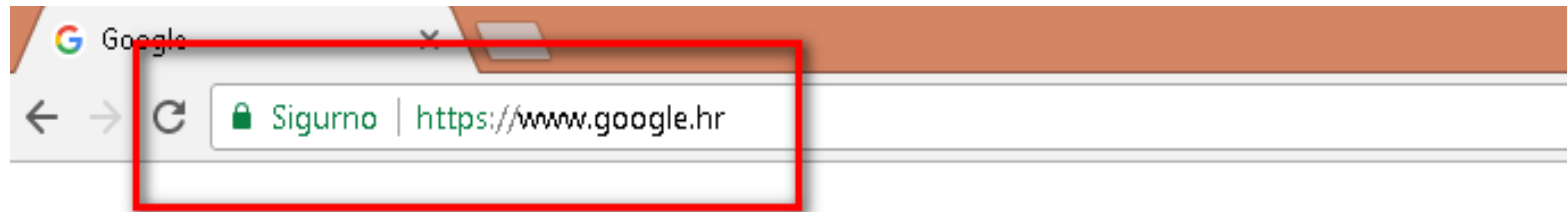
- Slanja poruka na internetu analogno je slanju klasične pošte.
- Osnovno princip – šifriranje podataka.
- Temeljni cilj – podizanje razine sigurnosti komunikacije

Osnove Internet sigurnosti



[Ta fotografija](#) korisnika Nepoznat autor: licenca [CC BY-SA](#)

Osnove Internet sigurnosti



- Primjer: web lokacija s kojom sigurno komuniciramo.
- Mora se koristiti HTTPS protokol.

Prijetnje privatnosti i identitetu

- krađa identiteta
- Kako dolazi do krađe identiteta?
- Što poduzeti da se zaštitimo?




Izvor: ucomics.com

Phishing



finamhch@business28.web-hosting.com on behalf of FINA.hr <tomislav.horvat@fina.online>

Elektronička obavijest o pokretanju ovršnog postupka

 We removed extra line breaks from this message.

Poštovani,

temeljem članka 3. Ovršnog zakona (NN 112/12, 25/13, 93/14, 55/16, 73/17), točka 6., obavještavamo Vas o pokrenu

Prijedlog ovrhovoditelja možete preuzeti putem sljedeće poveznice:

https://www.fina.online/ovr/Prijedlog_za_ovrhu_urbr_220-2017.pdf

Napominjemo da možete, sukladno članku 162. Ovršnog zakona, točna 2., nakon što primite rješenje o ovrsi, predložiti žalbu. O prijedlogu za odgodu ovrhe podnesenom u roku za žalbu protiv rješenja o ovrsi sud će odlučiti u roku od 8 dana. Odmah dostaviti Agenciji u pisanom otpravku, a u slučaju potrebe priopćiti i telefaksom, elektroničkom poštom ili na drugi način.

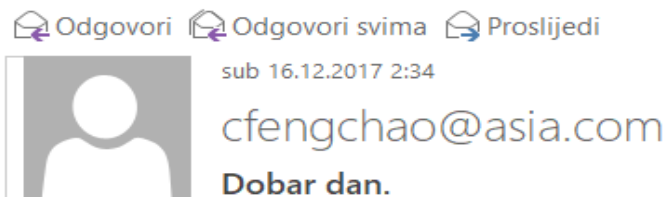
Srdačan pozdrav

Tomislav Horvat

FINA - Financijska agencija

Sektor financijskih i elektroničkih usluga Ovršni odjel Ulica grada Vukovara 70, 10 000 Zagreb tel 01 6127 016 fax 01 6127 017

Primjer **prijetnje** putem elektroničke pošte



Prima ☐ Recipients

i 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 filter za bezvrijednu e-poštu programa Outlook.

Dobar dan,

Ja sam izvršni direktor u industrijskoj i trgovačkoj banci Kine (ICBC). Imam zajednicki poslovni prijedlog koji se odnosi na racun u inozemstvu, uz vašu pomoc kao stranog partnera kao korisnika sredstava. Sve o ovoj transakciji obaviti ce se legalno u mojoj zemlji i vašoj. Ako ste zainteresirani, odgovorite putem moje privatne e-pošte navedene u nastavku i dati ću vam vaš pozitivan odgovor.

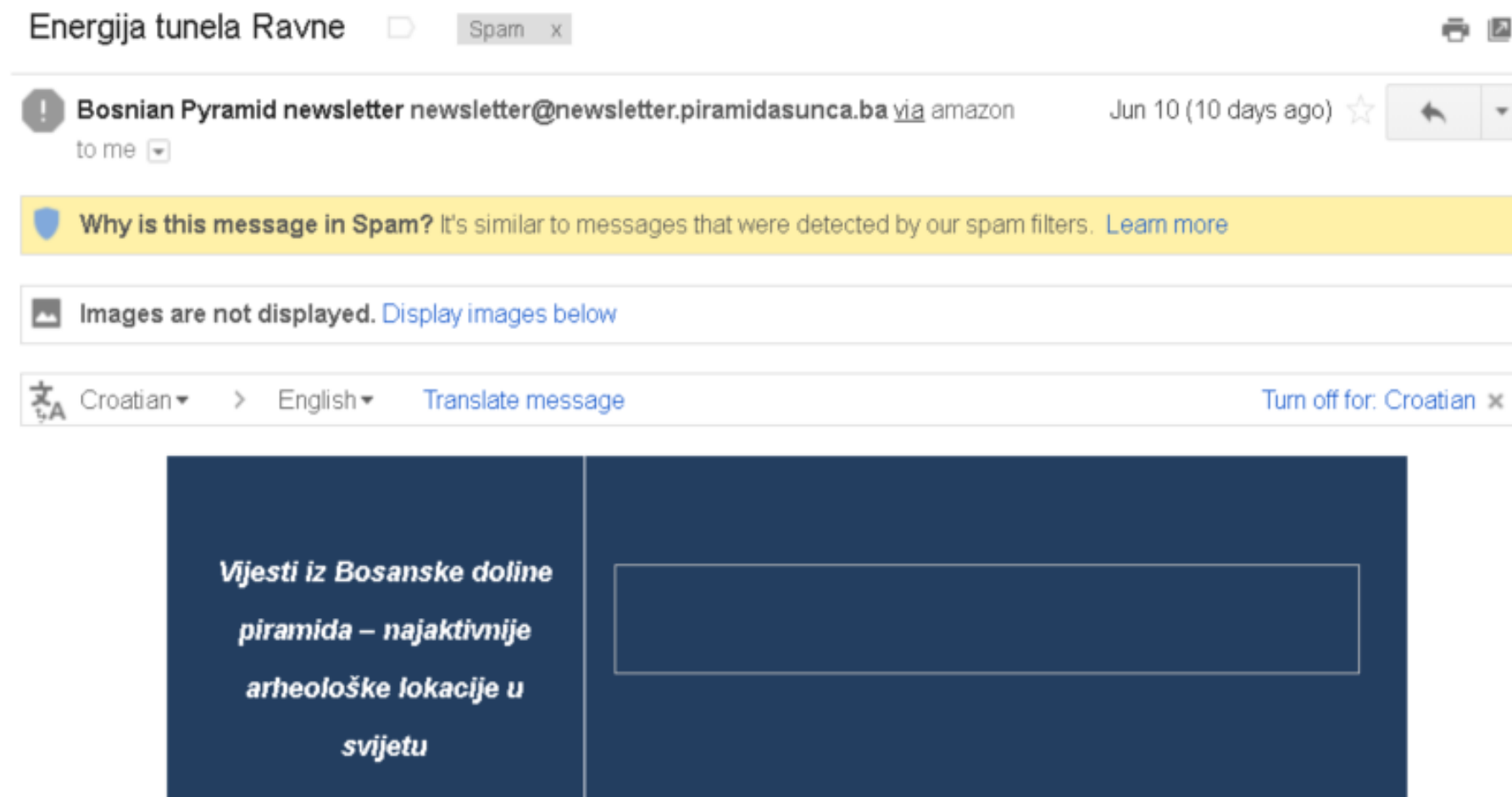
Privatna e-pošta: director.cfengchao@gmail.com

Lijepi Pozdrav,

Izvršni direktor.

ICBC .China

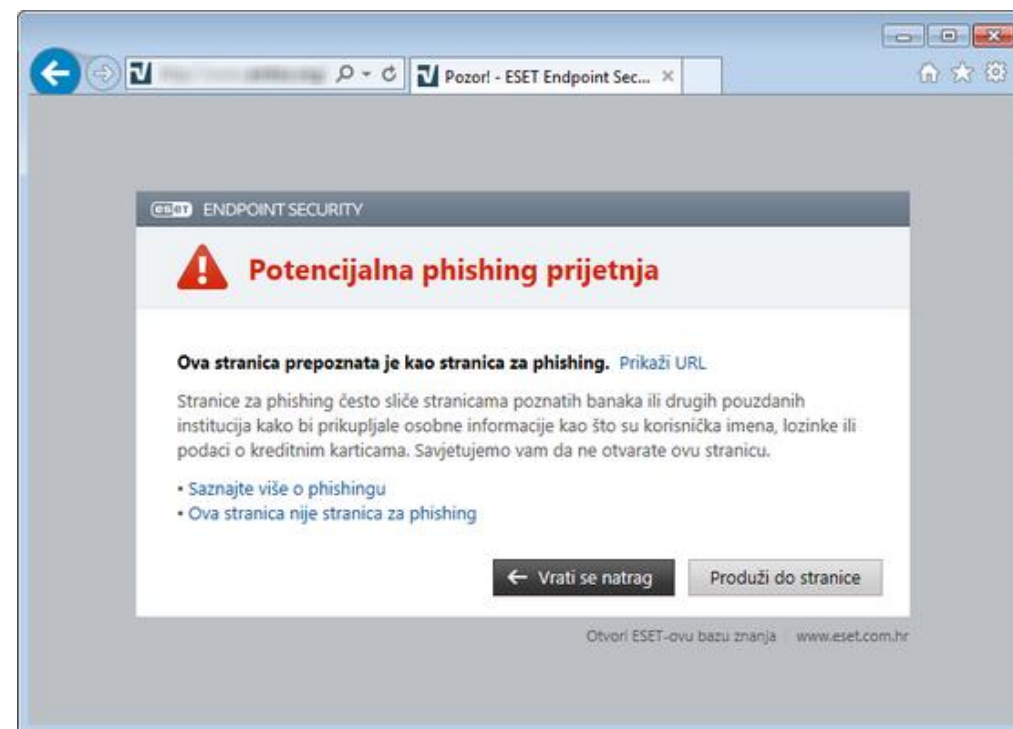
SPAM – neželjena elektronička pošta



Kako se zaštititi od phishinga i krađe identiteta



Izvor: [IBM](#)



Izvor: [ESET antiphishing zaštita](#)

U slučaju zlouporabe osobnih podataka ili krađe identiteta

- Kontaktirati policiju i predočiti dokaze koje smo sakupili (elektroničke poruke, eventualni ugovori, web lokacije...).
- Ako je riječ o ugovorima s tvrtkama koje je netko u vaše ime sklopio – kontaktirati i pružatelja ugovorene usluge.
- Kontaktirati i Agenciju za zaštitu osobnih podataka (AZOP).

Prijetnje pomoću društvenih mreža

Suggested Post ...

 **FireEye, Inc.** Sponsored • 

Gain unique insights into what to expect from attackers, victim organizations, security vendors & nation-states in the coming year



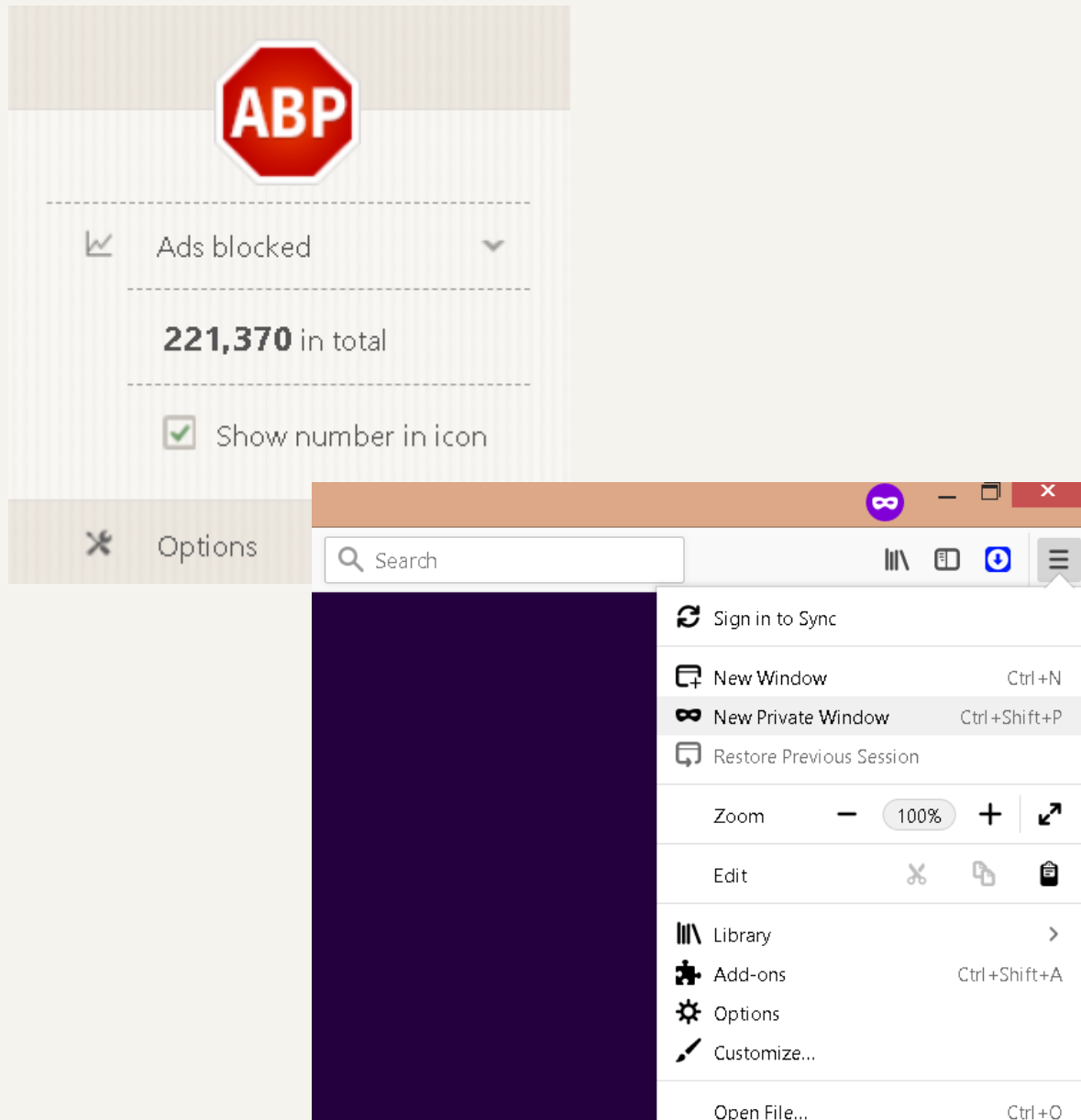
 FireEye

FIREEYE.COM
FireEye® Security Predictions 2018
Download your Copy Today!

LIKE PAGE

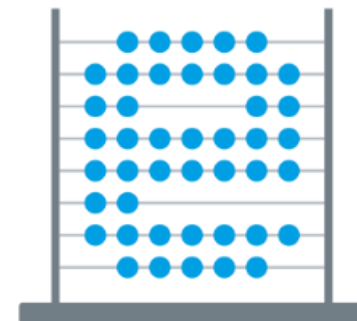
DOWNLOAD

- Svi ostavljamo podatke o sebi i svojim aktivnostima na servisima kao na Twitter i Facebook, koji ih kasnije koriste za ciljane oglase.
- Zlonamjerni korisnici ušli su i u taj segment života i žele ostvariti novčanu ili neku drugu korist



Kako se zaštititi

- postoji mnoštvo alata za zaštitu privatnosti
- AdBlocker Pro, korišćenje privatnih prozora
- potražite savjet službe za tehničku pomoć i sl.



e-Škole

Digitalni identitet

Digitalni identitet

- Digitalni identitet i digitalni trag su skup informacija dostupnih o nekoj osobi putem interneta.
- Privatni i javni identitet.

Privatni digitalni identitet

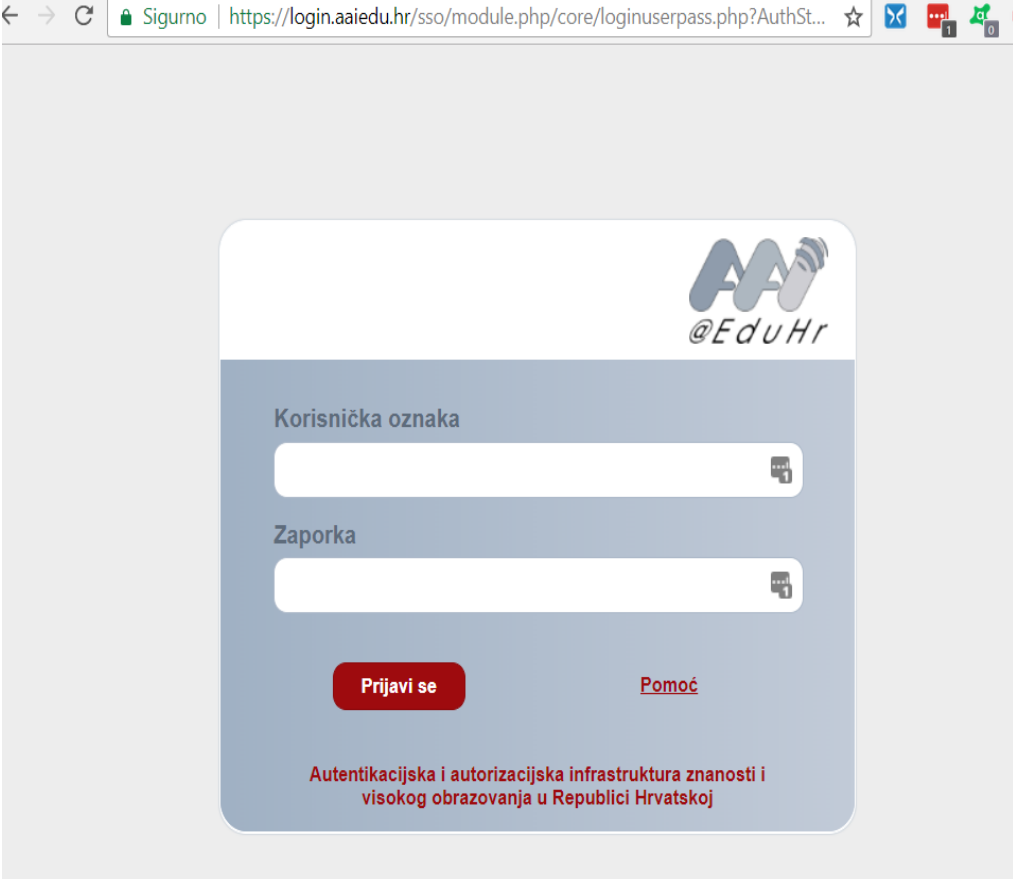
- Omogućuje pristup poslovnim sustavima.
- Aktivnosti na sustavu i unošenje podataka vidljive samo onima koji imaju prava.
- Elektronički identitet u sustavu AAI@EduHr
- Primjer:
 - e-Građani
 - Office 365 za škole
 - sustav za udaljeno učenje.

- Sadržaj koji:
 - stvaramo sami, gledajući sadržaje na internetu, preuzimajući dokumente i sl.
 - stvaraju naši prijatelji, kolege i poznanici kada ostave informacije o nama.
- Podatke možemo ostavljati namjerno ili slučajno.

Javni
digitalni
identitet

Sigurnost

- Izbjegavati pristupanje s javnih računala.
- Pripaziti da korisničko ime i lozinku upisujemo samo na stranici koja ju je izdala (npr. Ivan.Horvat@skole.hr upisivati samo na AAI@EduHr sustavu za prijavu!).
- Izgled login servisa sustava AAI@EduHr.

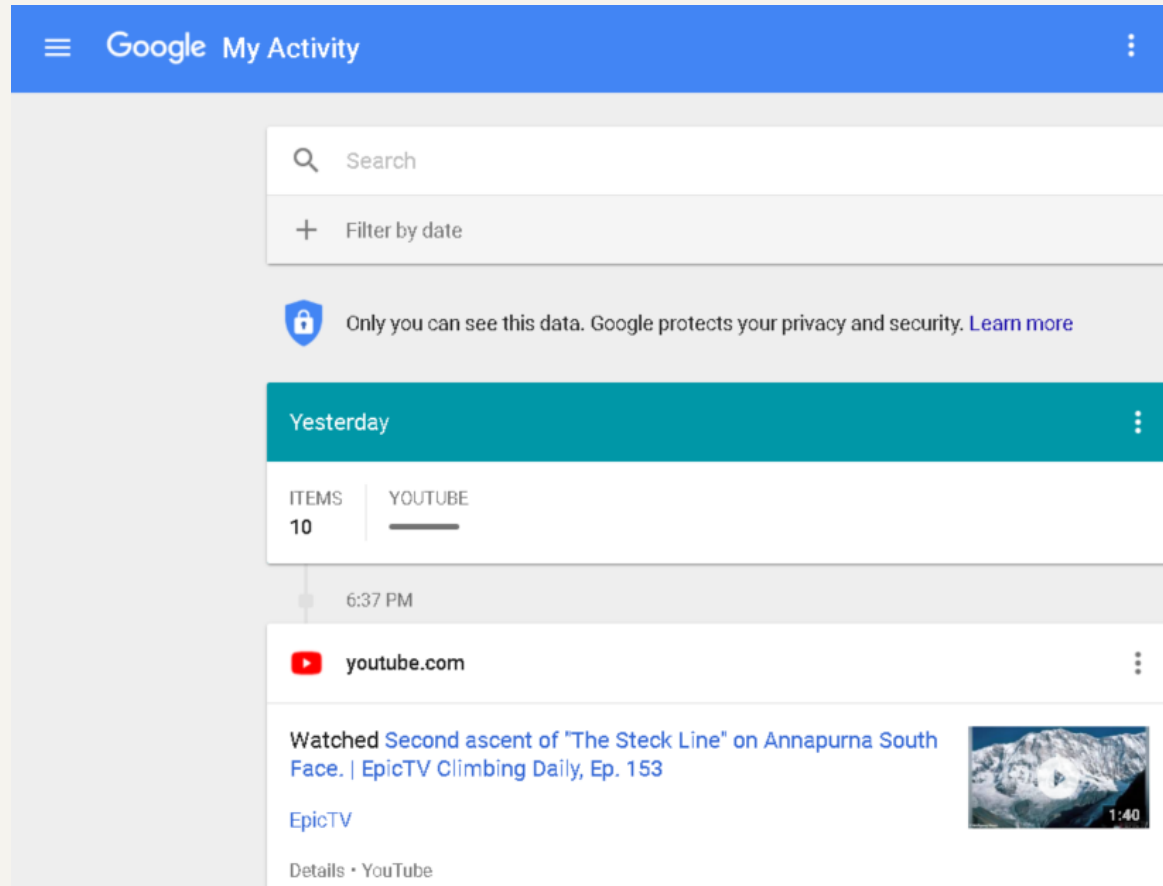


The screenshot shows a web browser window with the address bar displaying "Sigurno | https://login.aaiedu.hr/sso/module.php/core/loginuserpass.php?AuthSt...". The main content area features a login form with the AAI@EduHr logo at the top right. The form includes two input fields: "Korisnička oznaka" (User ID) and "Zaporka" (Password). Below the password field is a red "Prijavi se" (Login) button and a red "Pomoć" (Help) link. At the bottom of the form, there is a red text line: "Autentikacijska i autorizacijska infrastruktura znanosti i visokog obrazovanja u Republici Hrvatskoj".

Što sve internet zna o meni?

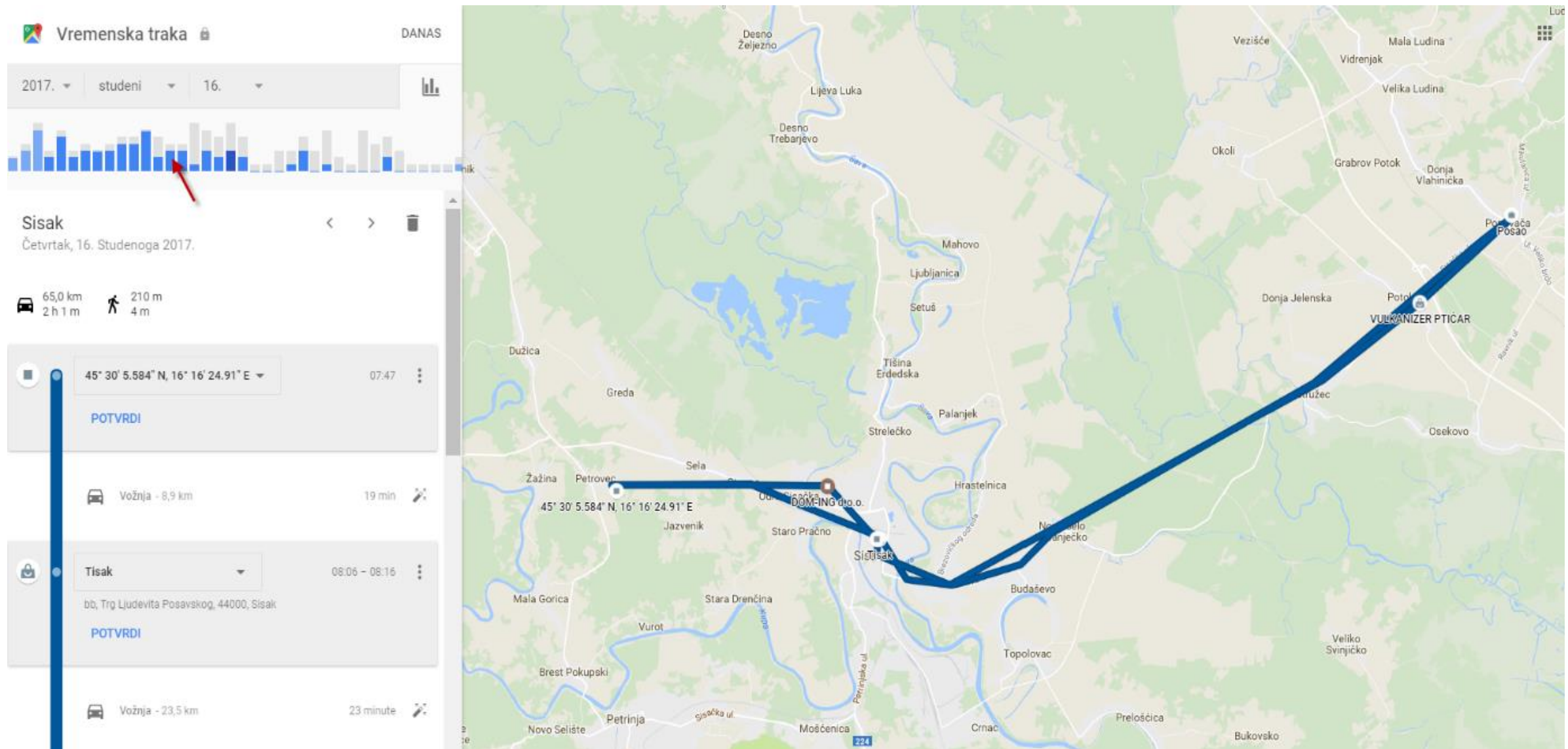
- Koje sve informacije internet zna o vama?
- Sve više korisnika ipak pazi što je od podataka javno dostupno.
- Ne koristite isti korisnički račun (Pogotovo ne lozinku!) za različite (internetske forume i elektroničku poštu) jer može dovesti do krađe identiteta.

Primjer: Google



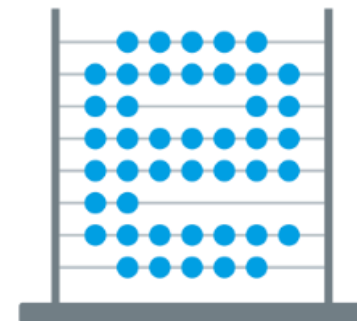
- Ako Vam netko ugrade pristupne podatke bit će u mogućnosti vidjeti:
 - povijest pretraživanja
 - korištene uređaje
 - vaše aktivnosti na internetu
 - vaš potrošački profil
 - povijest vašeg kretanja
 - koje aplikacije koristite.

Google vremenska traka



Zaštita

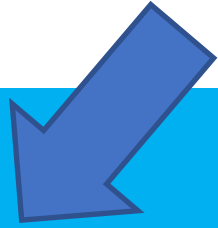
- Uključivanje anonimnog načina pretraživanja.
- Brisanje kolačića i povijesti pregledavanja.
- Podešavanje postavi privatnosti na uslugama koje koristimo.
- Promjena lozinki.
- Ne koristiti pamćenje lozinki na autorizaciju na stranice na internetu.



e-Škole

Fizička i elektronička zaštita digitalnog sadržaja

Fizička i elektronička zaštita



Fizička

- brave, sustavi kontrole prolaza, videonadzor i višestruka autentifikacije za ulaz u osjetljive prostorije

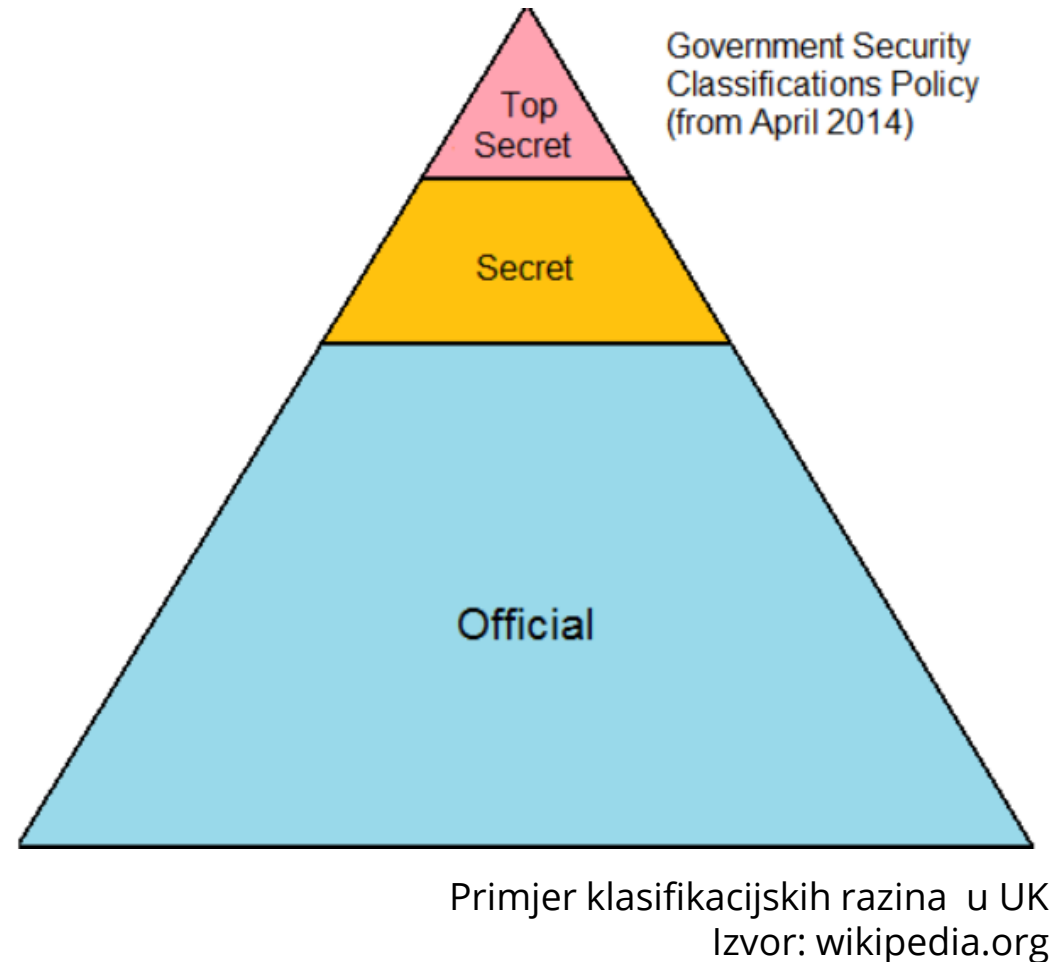


Elektronička

- Vatrozid, sustavi za detekciju i prevenciju intruzije, dozvole za korištenje mrežnih tehnologija za izolaciju prometa, dodjela najmanjih privilegija

Tajnost i klasifikacija podataka

- Tajnost podataka – zaštititi podatke adekvatnim mehanizmima i pristup dodijeliti po principu najmanjih privilegija.
- Klasifikacija podataka – označavanje dokumenata (pisanih i digitalnih) oznakama o tajnosti.



Pravilnih o sigurnoj i odgovornoj uporabi IKT

- Veća sustavna upotreba IKT-a odgojno-obrazovnih djelatnika i učenika.
- Rizici i prijetnje kojima smo izloženi korištenjem IKT-a.



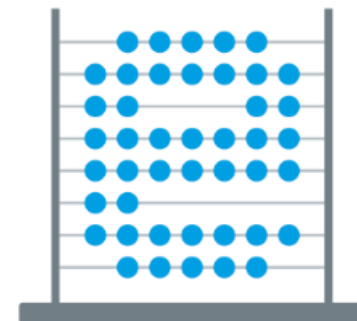
- **Prijedlog strukture Pravilnika o sigurnoj i odgovornoj uporabi informacijsko-komunikacijske tehnologije.**

Osnovni elementi Pravilnika

- Uvod
- Osnovne sigurnosne odredbe
- Škola IKT oprema i održavanje
- Reguliranje pristupa IKT opremi
- Sigurnost korisnika

Prihvatljivo i odgovorno korištenje informacijsko- komunikacijske tehnologije

- Ponašanje na Internetu
- Autorsko pravo
- Dijeljenje datoteka
- Internetsko nasilje
- Korištenje mobilnih telefona



e-Škole

Zaštita privatnosti i zakonski okviri zaštite privatnosti

Privatnost i osobni podaci

- Što je privatnost?
- Vrste privatnosti
 - fizička privatnost
 - informacijska privatnost
- Što su osobni podaci?

Primjeri osobnih podataka

- adresa fizičke osobe
- broj telefona
- e-mail adresa
- osobna fotografija
- identifikacijski broj/OIB
- biometrijski podaci (otisak prsta, snimka šarenice oka)
- podaci o obrazovanju i stručnoj spremi
- podaci o plaći
- podaci o kreditnom zaduženju
- podaci o računima u banci

Zaštita privatnosti na internetu

-

- Izbjegavati ostavljanje podataka koji nisu uvjet za korištenje usluga.
- Ne dijeliti tuđe osobne podatke bez pristanka.
- Ne vjerovati svemu što piše na internetu.

+

- Pročitati uvjete i korištenje usluge („sitna slova”).
- Koristiti sigurne i kompleksne lozinke.

Zaštita privatnosti djece

- S obzirom na veliku dostupnost informacija i drugačije navike mlađih generacija, tipičan problem.
- Sigurnosne politike i edukacija – jedini način da se djeca zaštite.
- Nemoguće je napraviti savršenu zaštitu privatnosti za djecu.
- Smanjiti količinu dostupnog sadržaja.

Sigurne lozinke

- Veće od 8 znakova.
- Koriste više skupina znakova
 - Velika (A-Z), mala slova (a-z), specijalni znakovi (!"#\$%), minimalna dužina 8 znakova
- Ne koriste istu lozinku za više različitih usluga.
- Bolje je koristiti dugačku lozinku punu riječi nego kratku koja je jako kompleksna.
- Redovito mijenjajte lozinke, ne koristite riječi ili često korištene izraze iz rječnika bilo kojeg jezika.
- Ne koristite riječi koje se relativno brzo mogu dovesti u vezu s vama (zanimanje, zaposlenje, poznanici...).

Zakonski okvir zaštite privatnosti

- Ustav RH – Članak 37.
- Opća uredba o zaštiti osobnih podataka
- Agencija za zaštitu osobnih podataka

Zaključak

- O zaštiti digitalnog sadržaja i osobnih podataka potrebno je neprestano razmišljati pri uporabi računala, bez obzira radi li se o osobnom ili poslovnom kontekstu.

- Važno je primjenjivati Model sveobuhvatne zaštite:
 - sigurnost računala, podataka i mreže
 - fizička sigurnost
 - primjena i razvoj politike i procedura zaštite i sigurnosti sadržaja i pojedinaca u digitalnom okruženju.
- **S napretkom tehnologija većina se stvari može prevenirati, ali samo pod jednim uvjetom, a to je da postoji svijest korisnika o potencijalnim opasnostima.**


Priručnik i prezentacija na Edutoriju u kolekciji


edutorij.e-skole.hr


NASLOVNICA MOJ EDUTORIJ MATERIJALI ▾ NAPREDNO PRETRAŽIVANJE KORISNICI ▾ O EDUTORIJU ▾

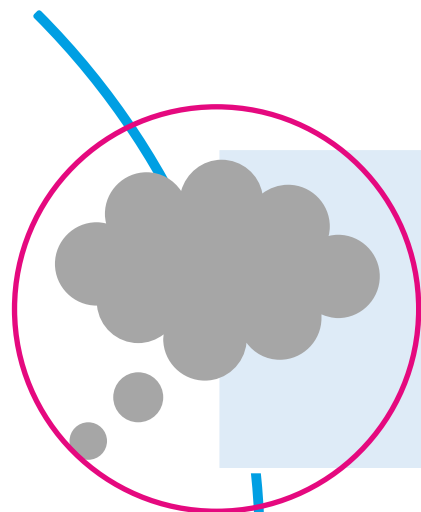
Unos novog materijala
Izrada nastavničke pripreme
Kolekcije
Digitalni obrazovni sadržaji - e-Škole
Scenariji poučavanja - e-Škole
Svi materijali

Istaknute kolekcije u Edutoriju:

 **Korisno o Edutoriju**
Korisni materijali o samom Edutoriju, te mogućnost komunikacije vezano uz Edutorij.

 **e-Škole obrazovanje korisnika (pilot projekt)**
Obrazovni sadržaji za provedbu obrazovanja korisnika razvijeni su u sklopu pilot projekta e-Škole (2015. -2018. g.), u okviru programa "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće" kojeg koordinira Hrvatska akademska i istraživačka mreža - CARNET. Sadržaji su usmjereni na razvoj digitalnih kompetencija odgojno-obrazovnih djelatnika škola.

 **e-Škole program obrazovanja (2. faza)**
Obrazovni sadržaji za provedbu obrazovanja korisnika razvijeni su u sklopu druge faze programa "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće" (2018. - 2021. g.) kojeg koordinira Hrvatska akademska i istraživačka mreža - CARNET. Sadržaji su usmjereni na razvoj digitalnih kompetencija odgojno-obrazovnih djelatnika školskih ustanova.



Evaluacija webinarara

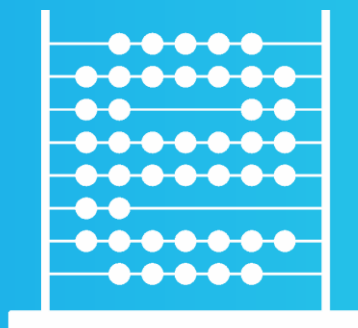
*Poveznica u Q&A panelu ili
skenirajte QR kod*



Potvrde o sudjelovanju u
aplikaciji za prijavu (EMA)

Kontakt edukacije u e-Škole projektu:
e-skole-edukacija@skole.hr

CARNET-ova korisnička podrška:
helpdesk@skole.hr



e-Škole

RAZVOJ SUSTAVA
DIGITALNO ZRELIH ŠKOLA
(II. FAZA)

Projekt je sufinancirala Europska unija iz europskih strukturnih i investicijskih fondova.
Više informacija o EU fondovima možete naći na web stranicama Ministarstva regionalnoga razvoja
i fondova Europske unije: www.strukturnifondovi.hr

Sadržaj ovog materijala isključiva je odgovornost Hrvatske akademske i istraživačke mreže - CARNET.

Kontakt: Hrvatska akademska i istraživačka mreža – CARNET | Josipa Marohnića 5, 10000 Zagreb
Tel.: +385 1 6661 616 | www.carnet.hr



Ovo djelo je dano na korištenje pod licencom Creative Commons
Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima
4.0 međunarodna.