FILOZOFSKI FAKULTET
SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI

Izv. prof. dr. sc. Anita Papić

Definicije i pojmovi iz područja informacijske sigurnosti

- **Informacijska sigurnost** – stanje povjerljivosti, cjelovitosti i raspoloživosti podataka koje se postiže primjenom odgovarajućih sigurnosnih mjera.
- **Kibernetički prostor** – prostor unutar kojeg se odvija komunikacija između informacijskih sustava. U kontekstu Strategije obuhvaća Internet i sve sustave povezane na njega.
- **Kibernetička sigurnost** – obuhvaća aktivnosti i mjere kojima se postiže povjerljivost, cjelovitost i dostupnost podataka i sustava u kibernetičkom prostoru.
- **Kibernetički (računalni) kriminalitet** – činjenje kaznenih djela protiv računalnih sustava, programa i podataka, počinjena unutar kibernetičkog prostora uporabom informacijskih i komunikacijskih tehnologija.
- **Kibernetička kriza** – događaj ili niz događaja u kibernetičkom prostoru, koji bi mogli uzrokovati ili su već prouzročili veći poremećaj u društvenom, političkom i ekonomskom životu RH. Takvo stanje u konačnici može utjecati na sigurnost ljudi, demokratski sustav, političku stabilnost, gospodarstvo, okoliš i druge nacionalne vrijednosti odnosno na nacionalnu sigurnost i obranu države općenito.

...

- **Osjetljivi podaci** – skupine podataka koje se koriste samo za službene potrebe ili skupine podataka koje su zaštićene odgovarajućim propisima, a pri tome nemaju svojstvo tajnosti (npr. označeni neklasificirani podaci ili osobni podaci).
- **Zaštićeni podaci** – podaci koji zbog svog sadržaja imaju osobit značaj za vrijednosti štićene u demokratskom društvu, zbog čega ih država prepoznaje kao osjetljive te ih razvrstava u različite skupine podataka za koje vrijede specifični zahtjevi postupanja u odnosu na svojstva podatka kao što su povjerljivost, cjelovitost, raspoloživost, odnosno privatnost.
- **Računalni sigurnosni incident** – jedan ili više računalnih sigurnosnih događaja koji su narušili odnosno narušavaju sigurnost informacijskog sustava.
- **Sigurnosne mjere** – opća pravila zaštite podataka koja se realiziraju na fizičkoj, tehničkoj ili organizacijskoj razini.
- **Sustav identifikacije i autentifikacije** – sustav kojim se utvrđuje i verificira identitet osoba, uređaja ili usluga na informacijskim sustavima.

CERT

Computer Emergency Response Team- uobičajena kratica za skupinu stručnjaka odgovornih za rješavanje sigurnosnih incidenata na računalnim mrežama.

(1) CERT je nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj.

(2) CERT je zasebna ustrojstvena jedinica koja se ustrojava u Hrvatskoj akademskoj i istraživačkoj mreži (CARNet).

(3) CERT usklađuje postupanja u slučaju sigurnosnih računalnih incidenata na javnim informacijskim sustavima nastalih u Republici Hrvatskoj, ili u drugim zemljama i organizacijama, kad su povezani s Republikom Hrvatskom.

(4) CERT usklađuje rad tijela koja rade na prevenciji i zaštiti od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj te određuje pravila i načine zajedničkog rada.

HR ISO/IEC 27000

- Skup međunarodnih normativnih dokumenata za područje upravljanja informacijskom sigurnošću, prihvaćen kao Hrvatska norma.

SEKTORI DRUŠTVA I OBLICI SURADNJE DIONIKA KIBERNETIČKE SIGURNOSTI

- **Javni sektor**
- **Akademski sektor**
- **Gospodarski sektor**
- **Građanstvo**

PODRUČJA KIBERNETIČKE SIGURNOSTI

(A) Javne elektroničke komunikacije

(B) Elektronička uprava

(C) Elektroničke financijske usluge

(D) Kritična komunikacijska i informacijska infrastruktura i upravljanje kibernetičkim krizama

(E) Kibernetički kriminalitet

(F) Zaštita podataka

(G) Tehnička koordinacija u obradi računalnih sigurnosnih incidenata

(H) Međunarodna suradnja

(I) Obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru

Zakon o informacijskoj sigurnosti

Područja informacijske sigurnosti za koja se propisuju mjere i standardi informacijske sigurnosti su:

- sigurnosna provjera,
- fizička sigurnost,
- sigurnost podatka,
- sigurnost informacijskog sustava,
- sigurnost poslovne suradnje.

Edukacija i obuka o računalnoj sigurnosti

- U svrhu osvještavanja javnosti o važnosti kibernetičke sigurnosti te poticanja odgovornog korištenja interneta, CARNET-ov Nacionalni CERT pokrenuo je nacionalnu kampanju "Veliki hrvatski naivci". Kampanja je dio projekta „GrowCERT – Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini" koji je sufinanciran sredstvima Europske komisije putem Instrumenta za povezivanje Europe (CEF – Connecting Europe Facility).
- Svake godine u listopadu obilježava se Europski mjesec kibernetičke sigurnosti.

www.naivci.hr

https://naivci.hr/#Aktivnosti

Izvor:

- NACIONALNA STRATEGIJA KIBERNETIČKE SIGURNOSTI, URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_10_108_2106.html
- Zakon o informacijskoj sigurnosti, URL: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html

csi.hr

FILOZOFSKI FAKULTET
SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

Centar za sigurniji internet

Izv. prof. dr. sc. Anita Papić

Centar za
Sigurniji
Internet

Što je e-nasilje?

- Nasilje putem interneta (cyberbullying) obuhvaća situacije u kojima je dijete ili mlada osoba izloženo napadu drugog djeteta, tinejdžera ili grupe djece, putem interneta ili mobilnog telefona.
- Međuvršnjačko nasilje putem interneta uključuje poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijeđanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara. Može uključivati slanje okrutnih, zlobnih, katkad i prijetećih poruka, kao i kreiranje internetskih stranica koje sadrže priče, crteže, slike i šale na račun vršnjaka.
- Sve veći broj djece i mladih je izloženo vršnjačkom nasilju preko interneta, no zabrinjava činjenica da i dalje ono nije prepoznato kao ozbiljan problem u društvu. Jedan od razloga zbog kojih ovaj trend nije zabrinjavajuć leži u činjenici da se on događa u virtualnom svijetu te da nije prisutan u „stvarnom djetetovom okruženju“. Nažalost, ovaj problem je itekako prisutan u djetetovom životu i utječe na sva područja djetetovog funkcioniranja.
- Prije razvoja modernih tehnologija vršnjačko nasilje se događalo na igralištima, u parkovima, na hodnicima škole i bilo ga je moguće puno lakše opaziti i na njega reagirati. Danas se sve događa u „virtualnom svijetu“, no to ne umanjuje ozbiljnost ovog problema. Dijete ili mlada osoba i dalje mogu biti izloženi različitim oblicima nasilja, i dalje u tome mogu sudjelovati i druga djeca koja možda neće preuzeti ulogu zlostavljača, ali neće ni spriječiti nasilje, ali ono što posebno zabrinjava je činjenica da dijete od ovog nasilja NE MOŽE POBJEĆI i ono nikad ne prestaje.
- Dijete svakodnevno „nosi svog zlostavljača u džepu“ zbog čega je vršnjačko nasilje putem interneta posebno zabrinjavajuće. Posljedice nasilja preko interneta katkad mogu biti i ozbiljnije od onih prouzročenih međuvršnjačkim nasiljem u stvarnim situacijama jer publika može biti puno veća, a zbog anonimnosti počinitelji mogu biti okrutniji i nasilniji nego što bi bilo u stvarnom svijetu.

Oblici e-nasilja

OBLIK NASILNOG PONAŠANJA	KRATKI OPIS
Izravan napad	Uključuje slanje uznemirujućih poruka, krađu ili promjenu lozinki, krađu ili promjenu nadimaka, objavu privatnih podataka ili neistina, slanje uznemirujućih slika, postavljanje internetske ankete o žrtvi, slanje virusa, slanje pornografije i neželjene pošte, lažno predstavljanje, poticanje grupne mržnje, napade na privatnost, uznemiravanje, uhođenje, vrijeđanje, nesavjestan pristup štetnim sadržajima te širenje nasilnih i uvredljivih komentara.
Napad preko posrednika	Uključuje napad počinitelja na žrtvu preko treće osobe koja toga najčešće nije svjesna.
Verbalno nasilje	Namjerno korištenje uvredljivih riječi s ciljem nanošenja psihološke povrede drugoj osobi (npr. vrijeđanje, nazivanje ružnim imenima, psovanje, izazivanje straha prijetnjama).
Relacijsko nasilje	Manipuliranje vršnjačkim odnosima s ciljem uništavanja osjećaja prihvaćanja, prijateljstva i pripadanja, odnosno usmjereno je na isključenje žrtve iz vršnjačkog društva (npr. ne uključivanje osobe u grupne razgovore i aktivnosti).

...

Elektroničko seksualno nasilje	Predstavlja oblik nasilja koji uključuje slanje i dijeljenje sadržaja seksualne prirode koji služe za seksualno uznemiravanje druge osobe i zadovoljenje vlastitih seksualnih potreba. Elektroničko seksualno nasilje obuhvaća i objavljivanje i/ili prosljeđivanje intimnih slika i snimki bez pristanka osobe, širenje glasina koje se odnose na seksualni život žrtve, zadovoljenje pohote pred djecom ili mamljenje djece za zadovoljenje spolnih potreba, uključivanje djece u pornografske aktivnosti. Ovakvi sadržaji mogu sadržavati poruke, slike, komentare, video uratke te druge audio-vizualne materijale intimnog sadržaja (prikaz intimnog dijela tjela, prikaz spolnih odnosa, poruke seksualiziranog sadržaja).

Metode e-nasilja

Grubo online sukobljavanje	Kratkotrajna rasprava između dvije ili više osoba koju karakterizira ljut, eksplicitan i vulgaran govor, uvrede a ponekad i prijetnje. Počinitelj nasilja ima za cilj izazvati bijes, tugu i/ili poniženje kroz namjerno izazivanje sukoba
Uznemiravanje	Opetovano slanje okrutnih, uvredljivih, neprijateljskih i provokatvnih poruka pojedincu/ki ili grupi. Najčešće se događa putem privatnih poruka, a cilj počinitelja nasilja jeprijetećim radnjama dovest drugu osobu u ponižavajući i/ili podređeni položaj
Ogovaranje i klevetanje	Izmišljanje informacija o žrtvi s ciljem povrede osobe te njihovo elektroničko slanje i dijeljenje. Uključuje stavljanje slike lica osobe na nepoznato golo tjelo i dijeljenje te slike. Cilj ovih radnji je nanošenje štete žrtvinoj reputaciji ili uništavanje odnosa s drugim osobama
Lažno predstavljanje	Uzimanje tuđeg identiteta i slanje poruka i drugih sadržaja u tuđe ime.
Iznuđivanje i širenje povjerljivih informacija	Javno objavljivanje podataka koje je žrtva poslala počinitelju nasilnika u povjerenju. Također, počinitelj nasilja može izmanipulirati žrtvu da napiše nešto privatno što onda počinitelj nasilja javno objavljuje ili šalje dalje bez dopuštenja.

...

Socijalno isključivanje	Događa se jednako na Internetu kao i u offline svijetu. Žrtve ne mogu ući u određene chat sobe ili ih se ne uključuje u grupne poruke
Prijetnje i uhođenje	Opetovano slanje prijetećih poruka te neprestani pokušaji uspostavljanja i nastavljanja neželjenog kontakta zbog kojih se žrtva počinje bojat za vlasttu sigurnost i dobrobit. Posebno je izraženo prilikom komunikacije s nepoznatm osobama te u slučajevima seksualnog nasilja putem Interneta
Videosnimanje	Snimanje ili fotografiranje u situacijama koje su za djecu ponižavajuće ili neugodne; izazivanje i snimanje tučnjave ili drugih nasilnih sadržaja te njihovo širenje.
Izmjena fotografija	Izmjena osobnih fotografija bez dozvole i objava na internetu.

Pojmovi

CYBERBULLYNG – nasilje preko Interneta, općiје pojam za svaku komunikacijsku aktivnost cyber tehnologijom koja se može smatrati štetnom kako za pojedinca tako i za opće dobro. Tim oblikom nasilja među vršnjacima obuhvaćene su situacije kada je dijete ili tinejdžer izložen napadu drugog djeteta, tinejdžera ili grupe djece, putem interneta ili mobilnog telefona.

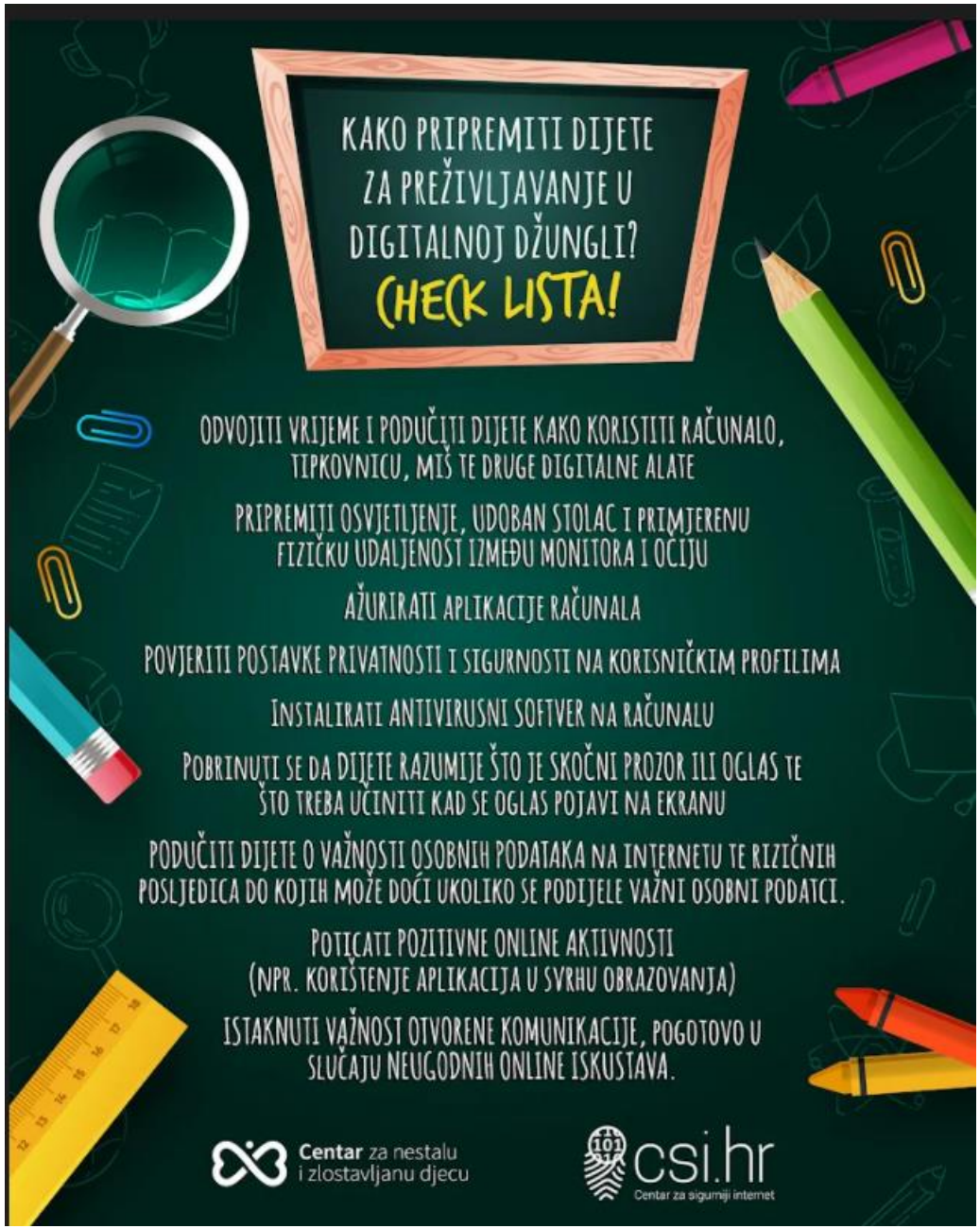
Neki primjeri cyberbullyinga su: širenje neugodnih informacija (istinitih ili lažnih), otvaranje grupe mržnje, nedopušteno objavljivanje nečijih fotografija ili videa, otvaranje lažnih profila, širenje uvredljivih komentara, krađa lozinke, namjerno isključivanje osobe iz grupe, uhođenje i uznemiravanje na internetu, kreiranje uvredljivih sadržaja na internetu o vršnjacima (priče, slike)

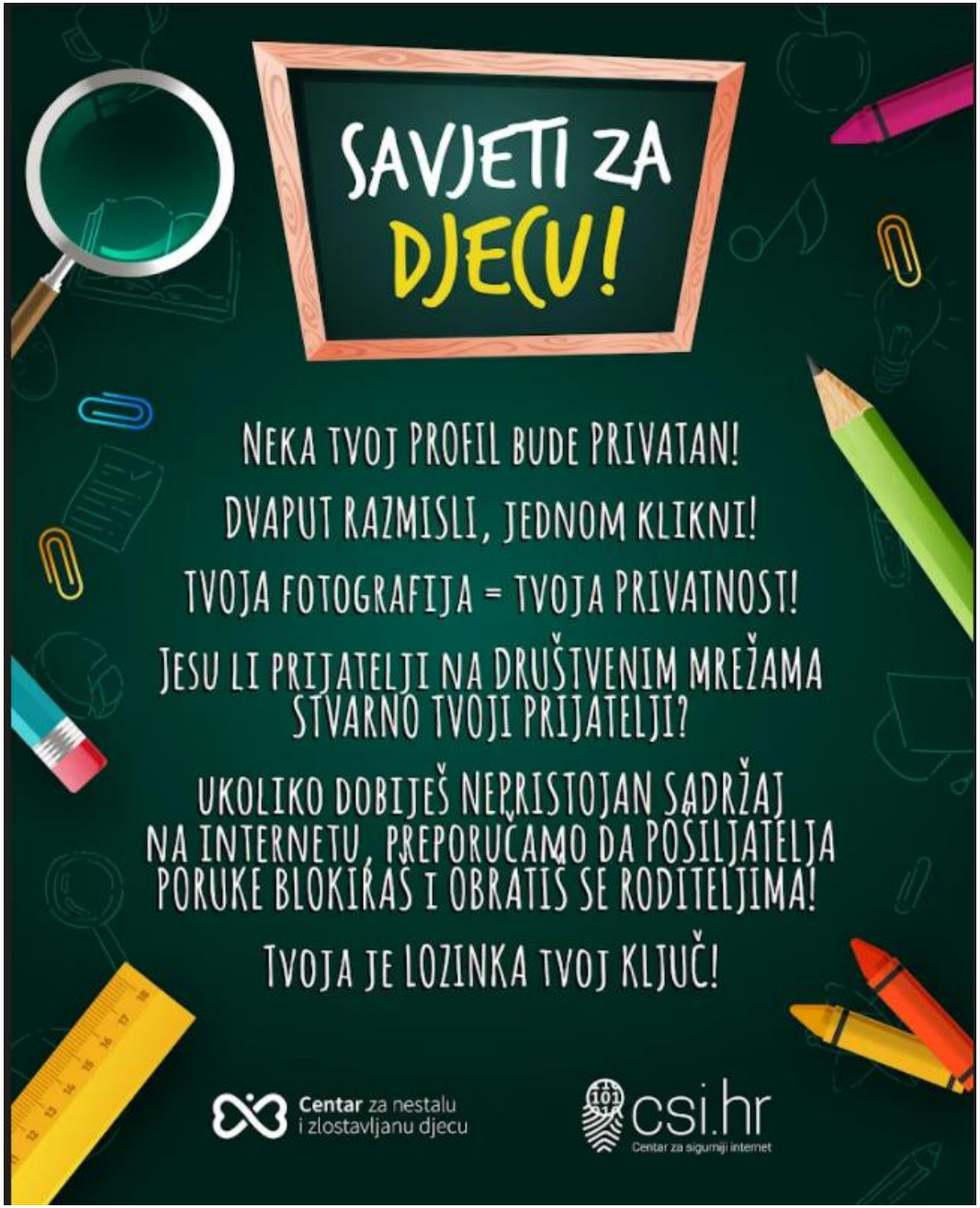
PHISHING - prijevara putem elektroničke pošte odnosno elektroničke poruke. Pošiljatelj navodi žrtvu da otkrije osobne informacije njihovim upisivanjem na lažnoj internetskoj stranici čija je poveznica dana u poruci, pri čemu su adresa i sadržaj te lažne stranice vrlo slični adresi i sadržaju neke autentične stranice.

GROOMING – odnosi se na situacije kada odrasla osoba uznemirava djecu putem SMS poruka, telefona ili Interneta. Tada se odrasla osoba predstavlja kao dijete, ulazi u komunikciju s njima i pokušava stvoriti osjećaj povjerenja kako bi razmjenili fotografije ili informacije seksualne prirode. Može tražiti dijete da mu pošalje svoju sliku, da mu opiše svoje tijelo, da mu otkrije svoje ljubavne tajne, ali i da se nađu u stvarnom životu.

IZNUĐIVANJE - Situacije u kojima osoba prisiljava dijete ili mladu osobu da djeluje ili misli na određen način kroz primjenu sile, prijetnji, ili zastrašivanja putem Interneta.

TROLLING - proizvodnja provokativnih postova s ciljem stvaranja sukoba i uništavanja konstruktivne rasprave.


KAKO PRIPREMITI DIJETE ZA PREŽIVLJAVANJE U DIGITALNOJ DŽUNGLI?
CHECK LISTA!
ODVOJITI VRIJEME I PODUČITI DIJETE KAKO KORISTITI RAČUNALO, TIPKOVNICU, MIŠ TE DRUGE DIGITALNE ALATE
PRIPREMITI OSVJETLJENJE, UDOBAN STOLAC I PRIMJERENU FIZIČKU UDALJENOST IZMEĐU MONITORA I OČIJU
AŽURIRATI APLIKACIJE RAČUNALA
POVJERITI POSTAVKE PRIVATNOSTI I SIGURNOSTI NA KORISNIČKIM PROFILIMA
INSTALIRATI ANTIVIRUSNI SOFTVER NA RAČUNALU
POBRINUTI SE DA DIJETE RAZUMIJE ŠTO JE SKOČNI PROZOR ILI OGLAS TE ŠTO TREBA UČINITI KAD SE OGLAS POJAVI NA EKRANU
PODUČITI DIJETE O VAŽNOSTI OSOBNIH PODATAKA NA INTERNETU TE RIZIČNIH POSLJEDICA DO KOJIH MOŽE DOĆI UKOLIKO SE PODIJELE VAŽNI OSOBNI PODATCI.
POTICATI POZITIVNE ONLINE AKTIVNOSTI (NPR. KORIŠTENJE APLIKACIJA U SVRHU OBRAZOVANJA)
ISTAKNUTI VAŽNOST OTVORENE KOMUNIKACIJE, POGOTOVO U SLUČAJU NEUGODNIH ONLINE ISKUSTAVA.
Centar za nestalu i zlostavljanu djecu
csi.hr
Centar za sigurniji internet


SAVJETI ZA DJECU!
NEKA TVOJ PROFIL BUDE PRIVATAN!
DVAPUT RAZMISLI, JEDNOM KLIKNI!
TVOJA FOTOGRAFIJA = TVOJA PRIVATNOST!
JESU LI PRIJATELJI NA DRUŠTVENIM MREŽAMA STVARNO TVOJI PRIJATELJI?
UKOLIKO DOBIJEŠ NEPRISTOJAN SADRŽAJ NA INTERNETU, PREPORUČAMO DA POŠILJATELJA PORUKE BLOKIRAŠ I OBRATIŠ SE RODITELJIMA!
TVOJA JE LOZINKA TVOJ KLJUČ!
Centar za nestalu i zlostavljanu djecu
csi.hr
Centar za sigurniji internet

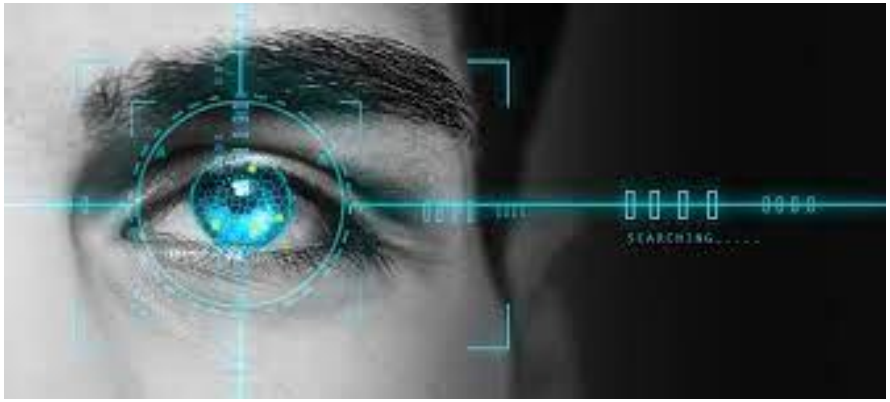
https://csi.hr/

- Video #lijepariječ
- Video Isprepletena priča
- Video Project Arachnid

FILOZOFSKI FAKULTET
SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU

Biometrija

Izv. prof. dr. sc. Anita Papić



Definicija biometrije

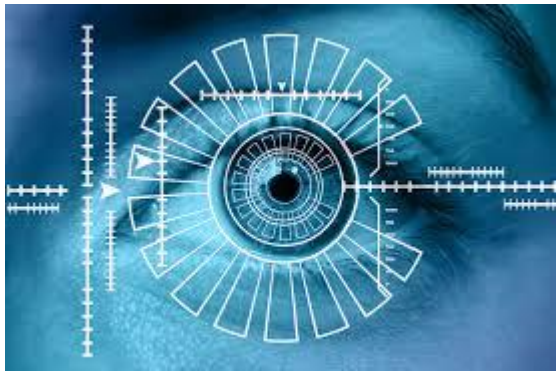
Prema prof. Miroslavu Bači biometrija predstavlja presjek nekoliko znanosti:

"… fizički i/ili ponašajni uzorak koji se može mjeriti i identificirati sa zadaćom potvrde identiteta osobe."

"… upućuje na automatsku identifikaciju osobe baziranu na njezinoj fizičkoj i/ili ponašajnoj karakteristici."

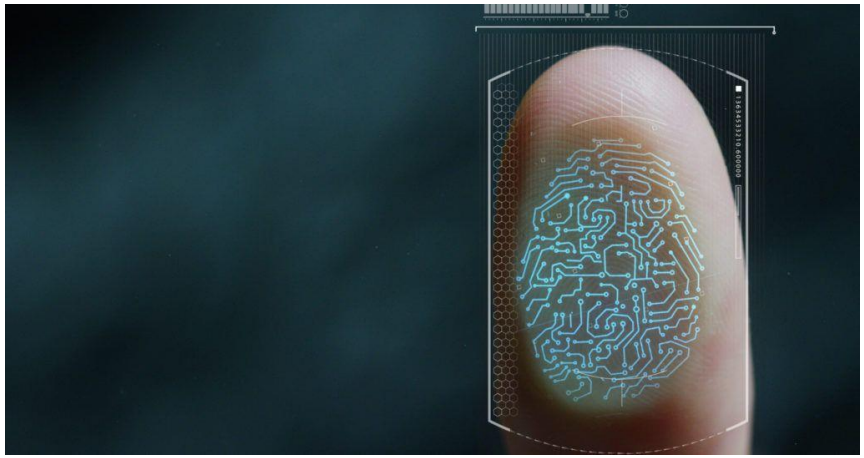
Biometrijske karakteristike

- “Tvrde”
- “Meke”
- Fizičke
- Ponašajne



Biometrijske metode

- Kontaktne
- Nekontaktne

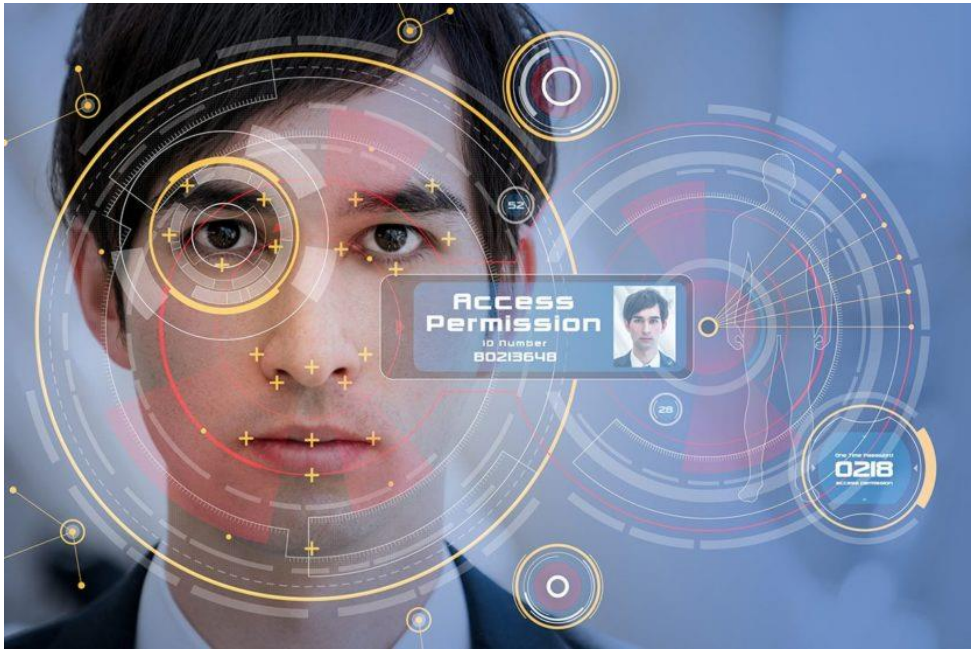


Identitet

- Identitet je skup značajki koje neku osobu čine onom koja jest
- Usporedba “jedan naprema više” 1:N

Verifikacija

- Testiranje korisnika radi potvrde da li je on/ona zaista osoba za koju se predstavlja
- Usporedba “jedan naprema jedan” 1:1



Biometrija i identitet

Identitet se često utvrđuje kroz:

- Nešto što osoba posjeduje (npr. iskaznica)
- Nešto što osoba zna (npr. PIN)
- Nešto što osoba jest (ljudsko tijelo)

Poteškoće

- Nešto što osoba posjeduje može se izgubiti
- Nešto što osoba zna može se zaboraviti
- Nešto što osoba jest …?

Pregled biometrijskih karakteristika

Fizičke

- Otisak prsta
- Slika lica
- Dlan
- Rožnica
- Šarenica
- Termogram lica/tijela
- Uho …

Ponašajne

- Potpis
- Glas
- Dinamika tipkanja
- Miris
- Hod …

…

“Tvrde”

- Otisak prsta
- Šarenica
- DNA
- Termogram lica

…

“Meke”

- Visina
- Boja kose
- Težina
- Boja očiju

…

…

Kontaktne

- Otisak prsta
- Dlan
- Rožnica
- Šarenica
- Potpis
- Hod

…

Nekontaktne

- Slika lica
- Glas
- Dinamika tipkanja
- Miris

…

Idealna biometrijska karakterstika

Univerzalnost

- Svaka osoba mora posjedovati tu karakterstiku

Jedinstvenost

- Dvije osobe ne smiju imati jednaku karakterstiku

Stalnost

- Mora biti stalna tijekom vremena

Prikupljivost

- Mora se moći prikupljati i mjeriti

Prihvatljivost

- Mora biti opće prihvaćena

Zahvaljujem na pozornosti!