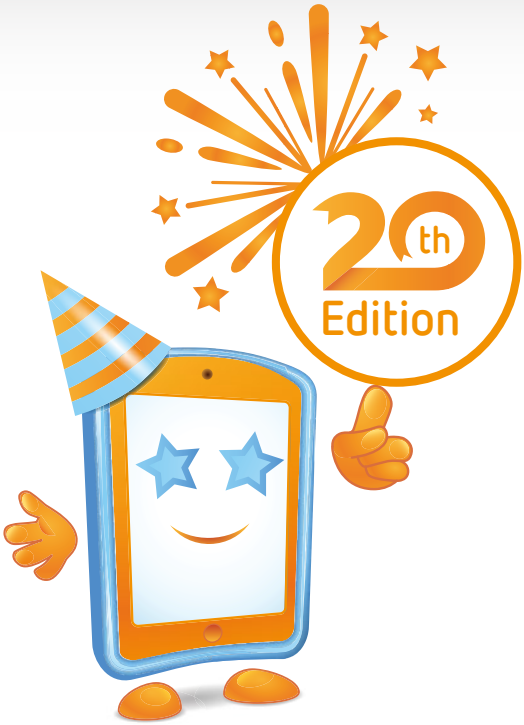
POJMOVNIK CENTRA ZA SIGURNIJI INTERNET



Dan Sigurnijeg Interneta 2023 | Utorak 7. veljače

Zajedno za bolji internet

www.dansigurnijeginterneta.org

European Commission

INHOPE

ins@fe

Centar za nestalu i zlostavljanu djecu

csi.hr
Centar za sigurniji internet

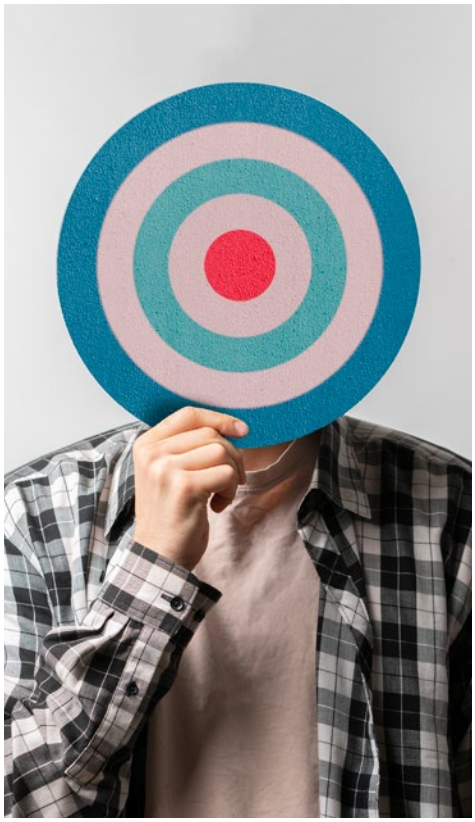
A1

ONLINE IZAZOVI

Korištenje TikToka i ostalih društvenih mreža može biti zabavno, uzbudljivo, a ponekad i edukativno. No kada su korisnici aplikacije osobe koje se uključuju u opasne trendove i izazove, do izražaja dolaze mračne strane online svijeta. Ne razmišljajući kritički o sadržaju, djeca i mladi ne mogu previdjeti opasnosti koje izazovi nose sa sobom.

KAKO POSTUPITI:

- rješenje nije oduzeti djeci mobitele i zabraniti im korištenje društvenih mreža
- razvijati odnos povjerenja s djecom, iskreno se zainteresirati za online svijet u kojemu žive
- educirati i sebe i djecu te prevenirati štetne posljedice
- razgovor s djecom o njihovom korištenju interneta - tko su im pratitelji na društvenim mrežama, poznaju li te ljude, za što najčešće koriste društvene mreže, postaviti obiteljska pravila o korištenju interneta
- prijavite neprimjerene sadržaje na društvenoj mreži na kojoj ih zateknete
- po potrebi prijavite slučaj policiji (ranije spremite dokaz)
- u slučaju bilo kakvih pitanja – obratite se Centru za sigurniji internet.



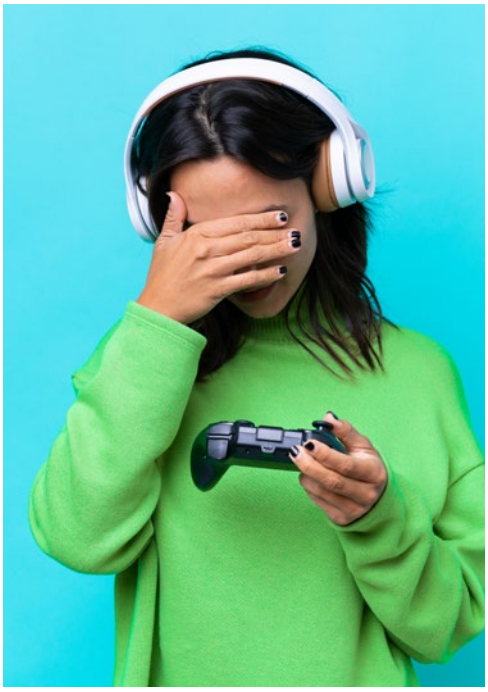
CANCEL CULTURE

Cancel culture ili kultura otkazivanja uključuje prestanak posjećivanja određenih korisničkih računa na društvenim mrežama, prestanak kupovine pojedinog proizvoda ili usluge te bojkotiranje novih glazbenih albuma ili filmova, prekide u suradnji i slično - ukoliko su se pokazali kontroverznima.

Pritisak kulture otkazivanja koji mladi stavljaju na osobe u javnom prostoru može pozitivno utjecati na osobe koje imaju određenu popularnost i platformu te na stavove koje javno iznose. Predstavlja i rizik od socijalnog isključivanja pojedinaca ukoliko se situacije vade iz konteksta, a osobu se socijalno izolira. Participacija mladih i poduzimanje aktivnih mjera s ciljem utjecaja na to kakvi sadržaji nam se javljaju u medijskom prostoru uvijek je pohvalna, no ne treba se zlorabiti.

POREMEĆAJ IGRANJA VIDEO IGARA

Dijagnozu Poremećaja igranja video igara karakterizira gubitak kontrole, poteškoće u funkcioniranju i pogoršanje ponašanja unatoč pojavi neugodnih posljedica na svakodnevni život.



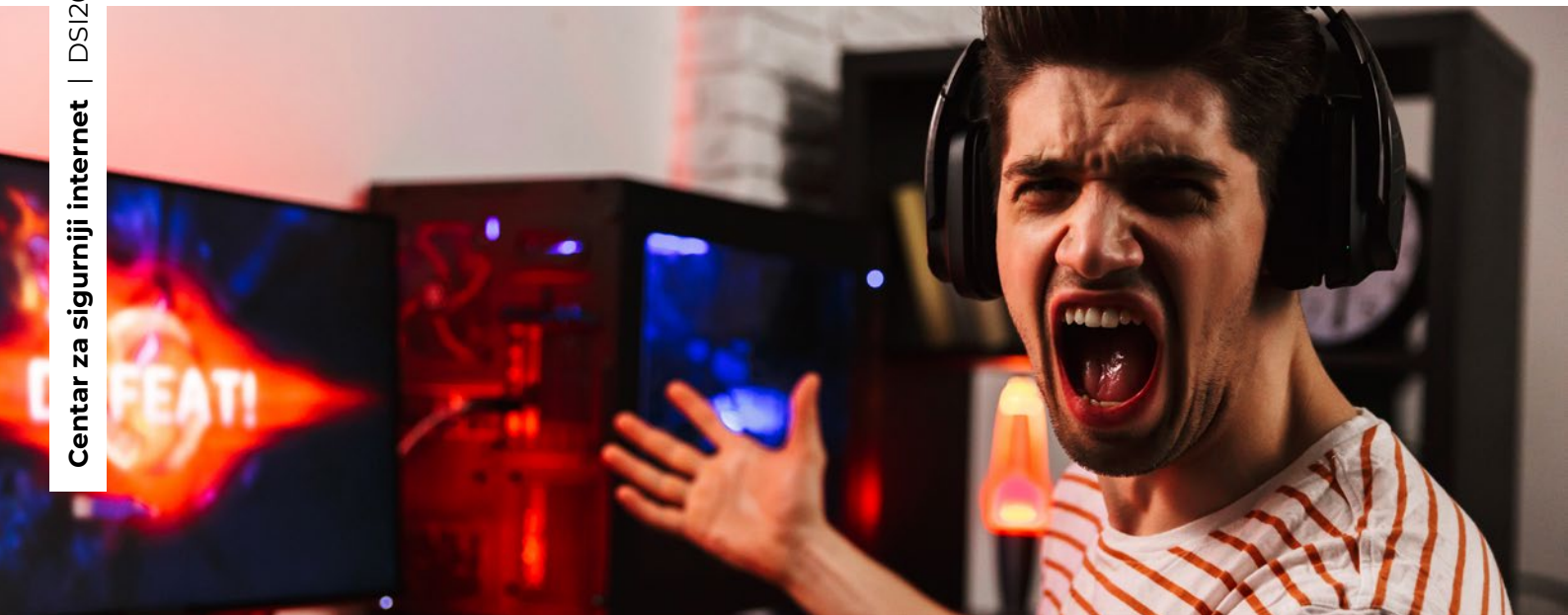
Uz to što još nema jasnih dijagnostičkih kriterija u dijagnostičkim priručnicima, stručnjaci navode da korištenje termina “ovisnost o internetu” dovodi do stigmatizacije, a što je najvažnije - šalje djeci poruku da ne možemo razumjeti njihovo ponašanje.

Ukoliko ste zabrinuti oko pretjeranog korištenja ekrana kod nekog djeteta, smatrate da je možda žrtva ili počinitelj elektroničkog nasilja, preporučujemo da se obratite stručnjacima mentalnog zdravlja u vrtiću/školi koje dijete pohađa.

FLAMING

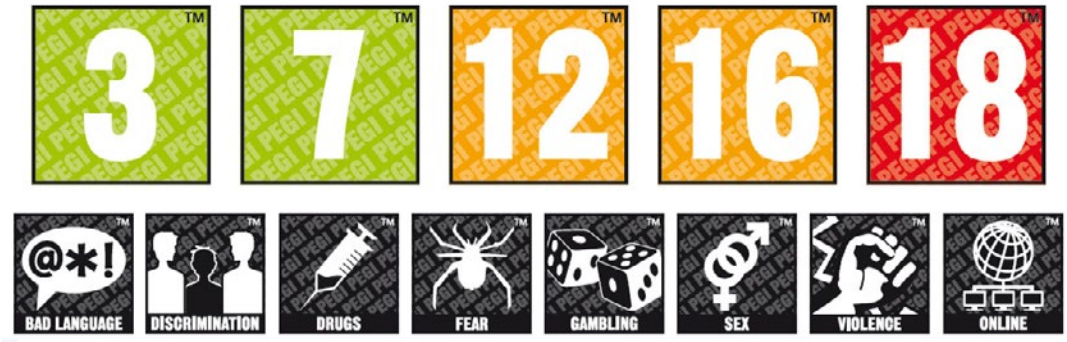
Slanje bilo kakvih neprimjerenih poruka koje potiču online sukobe. Iz ove je riječi proizašla i hrvatska inačica ‘’**flejmati**’’ koja se najčešće koristi u video igrama i to među igračima svih uzrasta, a odnosi se na vrijeđanje na temelju loših vještina u video igri. Tako vrijeđanje najčešće sadrži razne vulgarizme, a ponekad i govor mržnje.

Ovaj oblik neprimjerene komunikacije većinom ostaje unutar video igre, no i dalje može izazvati trajne posljedice. Kreatori video igara na ovaj problem utječu isključivanjem iz video igre, brisanjem korisničkog računa ili ograničavanjem mogućnosti korištenja chata.



PEGI OZNAKE

PEGI (The Pan-European Game Information) je sustav za rangiranje razvijen i dostupan svim članicama Europske unije. Glavni cilj programa je informiranje roditelja o donošenju odluka pri kupnji računalnih igara i stalno se ažurira novim igrama. Klasifikacije prema dobi djeteta prikazuju kojoj je dobnoj skupini igra, film, video, DVD i slično.



PREPORUKE ZA KORIŠTENJE DIGITALNIH UREĐAJA

Izbjeći korištenje ekrana u digitalnom dobu gotovo je nemoguće, no važno je poštivati granice. Postoji pregršt preporuka za korištenje ekrana ovisno o dobi djeteta, ali ono oko čega se slažu sve je da do dobi od oko 2 godine starosti djeteta nije preporučljivo izlagati djecu ekranima.

STRUČNJACI PREDLAŽU:

- do 2 godine - dijete ne treba biti izloženo zaslonima
- 2-5 godina - manje od 1 sat dnevno uz prisustvo roditelja
- 6-9 godina - 1 sat dnevno
- 10-12 godina - 1.5 sat dnevno
- 13-18 godina - 2 sata dnevno

Naglašavamo da je bitna i ravnoteža - što je dijete duže na računalu potrebno je i da provede više vremena u igri na zraku, bez računala.

DOBNO OGRANIČENJE ZA KORIŠTENJE DRUŠTVENIH MREŽA

Postoje kako bi se spriječilo prikupljanje osobnih podataka djece mlađe od 13 godina. Dobna granica od 13 godina nije slučajna - proizlazi iz američkog COPPA Zakona donesenog 1998. godine.

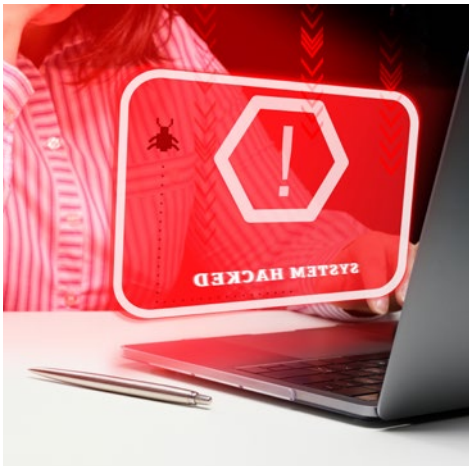
Neke su društvene mreže nakon europskog GDPR Zakona iz 2018. godine postavile dobnu granicu od 16 godina, a na drugim društvenim mrežama kao npr. Pinterestu dobna granica varira od 13 do 16 godina ovisno o državi u kojoj se nalazite.

Iako je dobna granica za kreiranje korisničkog računa na Youtube-u 13 godina, dobna granica od 18 godina postavlja se na videima koji se ocijene kao neprimjereni.

NESIGURNE WEB STRANICE

Rezultat pristupanja nesigurnim web odredištima može biti krađa osobnih podataka. Pojedine web stranice sadrže viruse koji uzrokuju poteškoće u radu digitalnih uređaja koji se koriste za pristupanje internetu. Otvaranjem nesigurne web stranice otvaraju se dodatni prozori i stranice koje nismo namjeravali otvoriti.

Kako prepoznati nesigurne web stranice:



- u poveznici nemaju https nego http ili se na početku poveznice ne pojavljuje lokot
- pretjerano prikazuju oglase u obliku skočnih prozora
- šalju sumnjive poruke, npr. Da ste osvojili nagradu ili da je na vašem računalu prisutan virus
- stranica nema politiku privatnosti, kontakt ni podatke o onome tko je takvu stranicu izradio

MEDIJSKA PISMENOST

Sposobnost pristupa medijima, razumijevanje i kritičko vrednovanje različitih aspekata medija i medijskih sadržaja te ostvarivanje komunikacije u raznovrsnim kontekstima. Kako unaprijediti medijsku pismenost?

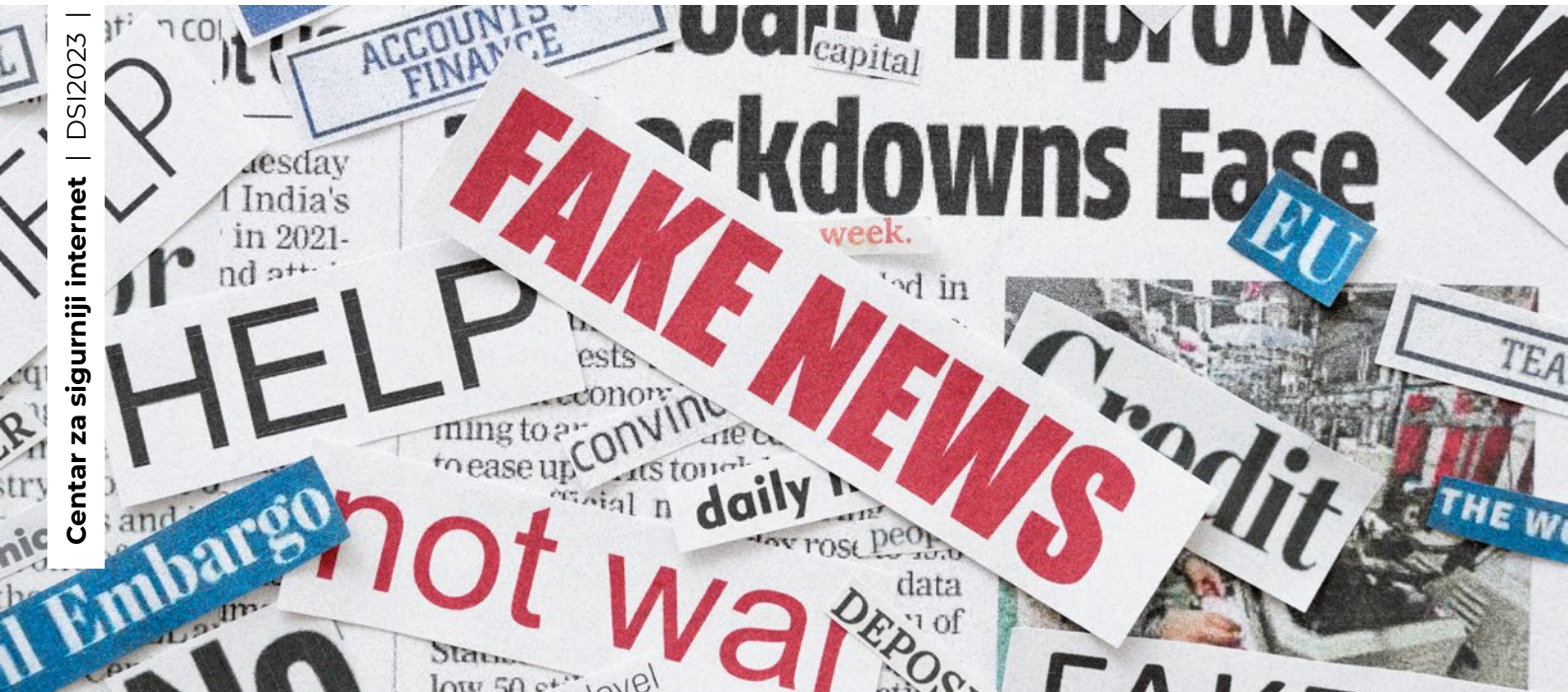
Velik dio današnjih interakcija odvija se na društvenim mrežama gdje nam je dostupna velika količina medijskog sadržaja. Treba imati na umu da su društvene mreže dostupne svakome te da svaki korisnik na njima može izraziti svoj stav. Zbog toga je važno raditi na kritičkom mišljenju - vrijedi pravilo: promislite dva puta prije donošenja zaključka na temelju pročitanog.

LAŽNE VIJESTI (FAKE NEWS)

Lažne vijesti odnose se na lažne ili krivo navodeće informacije koje se prezentiraju kao službene ili valjane. Objavljuju se iz više razloga, a neki od njih su širenje dezinformacija, zastrašivanje javnosti ili kao satira. Lažne vijesti ponekad se koriste i kako bi narušile reputaciju osobe o kojoj su objavljene.

Kako prepoznati lažne vijesti:

- obratite pozornost na izvor
- otvorite i pročitajte vijest, a ne samo naslov
- provjerite kada je vijest objavljena
- provjerite tko je autor i na koji je način povezan s temom



NEPRIMJERENA ONLINE KOMUNIKACIJA

Neprimjerena online komunikacija odnosi se na svaki oblik komunikacije u kojemu je namjera sramoćenje, nanošenje štete, omalovažavanje, dovođenje u opasnost i svaki drugi oblik komunikacije koji nepovoljno utječe na sudionike. Kada se susretnete s neprimjerenim sadržajem na internetu:

- Napravite snimku zaslona
- Prijavite sadržaj u aplikaciji u kojoj se nalazite
- Ukoliko ste zaprimili neprimjerenu poruku, osobi koja ju je poslala onemogućite daljnji kontakt s vama

Ukoliko se radi o ilegalnom sadržaju, prijavite ga bez odgode.

ONLINE NASILJE

Svaka zlonamjerna i ponavljana uporaba informacijskih i komunikacijskih tehnologija kako bi se nekome nanijela šteta, odnosno kako bi se najčešće neko dijete ponizilo, zadirkivalo, prijetilo mu se ili ga se zlostavljalo na neki drugi način.
Kako postupiti ako sumnjate na online nasilje:

- poduzeti sve potrebne mjere da se nasije prekine, a dijete zaštiti
- pružiti djetetu potrebnu pomoć i podršku
- prema potrebi i procjeni stručnjaka osigurati stručnu pomoć i podršku djetetu izvan škole ili ustanove socijalne skrbi

GOVOR MRŽNJE

Govor mržnje na internetu svaka je uporaba elektroničke komunikacijske tehnologije za širenje antisemitskih, rasističkih, fanatističkih, ekstremističkih ili terorističkih poruka ili informacija.

Što napraviti kada se susretnete s govorom mržnje:

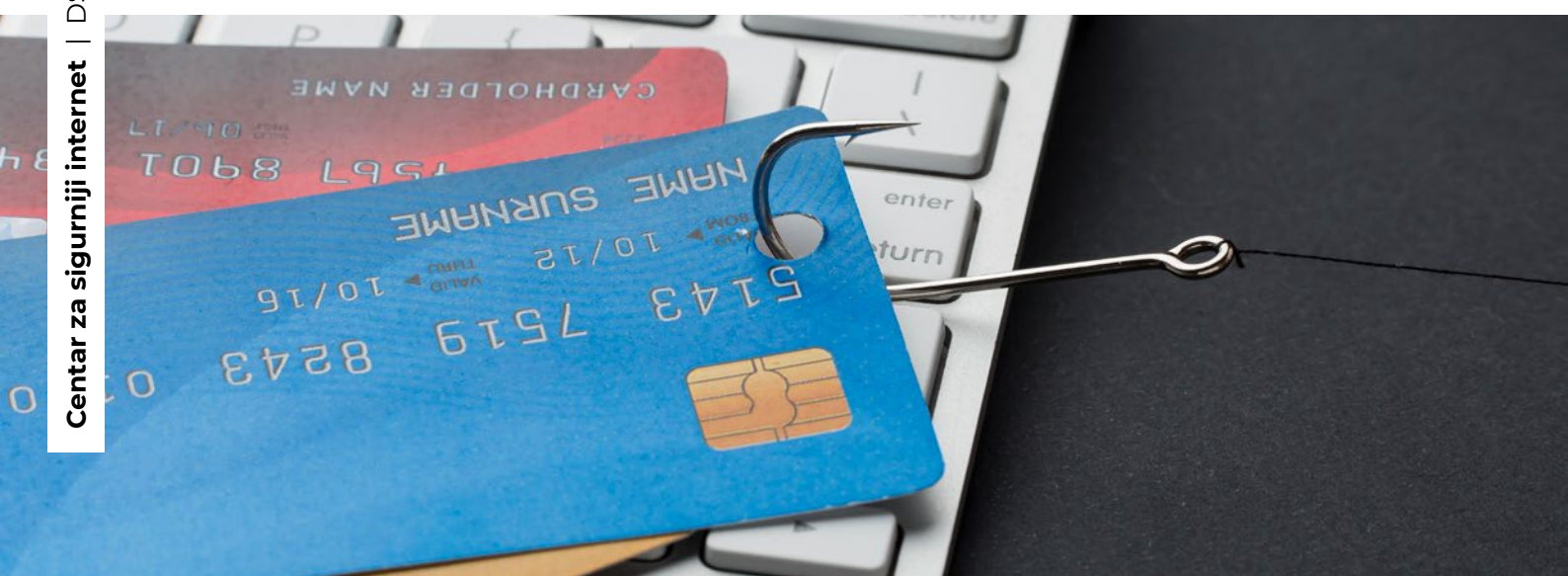
- napravite snimku zaslona
- prijavite komentar i/ili korisnički račun koji prenosi poruke koje sadrže govor mržnje
- ukoliko smatrate da je nečiji život ugrožen, kontaktirajte institucije

PHISHING

Phishing i druge prevare načini su na koje počinitelj pokušava doći do osobnih podataka, podataka za prijavu u neku aplikaciju ili novca. Može biti u obliku e-maila ili izravne poruke, a sve češće i u obliku poziva.

KAKO PREPOZNATI PHISHING:

- Sumnjive, dugačke, nepoznate ili pogrešno napisane poveznice, korisnička imena ili e-mail adrese
- Prijetnje ili zahtjevi kao npr. ''Ažurirajte do ponoći ili će Vaš račun biti zatvoren!''
- Pravopisne i/ili gramatičke pogreške
- Sadržaj zvuči predobro da bi bilo istinito
- Sve u čemu se traži prijava ili osobni podatci



HOTLINE I HELPLINE

Svakodnevnim provođenjem vremena na internetu susrećemo se s raznim situacijama za koje nemamo uvijek rješenje. Tada je poželjno potražiti pomoć stručnjaka.

ONLINE POMOĆ:

- **https://csi.hr/hotline/** - web stranica za prijavu ilegalnog sadržaja na internetu
- **0800 606 606** – besplatna anonimna savjetodavna linija, dostupna svakim radnim danom od 8 do 20 sati

HOTLINE

ANONIMNA PRIJAVA ILEGALNOG SADRŽAJA
WWW.CSI.HR/HOTLINE

HELPLINE

BESPLATNI I ANONIMNI TELEFON ZA POMOĆ I SAVJETOVANJE U SLUČAJU NASILJA NA INTERNETU
0800 606 606

csi.hr
Centar za sigurniji internet

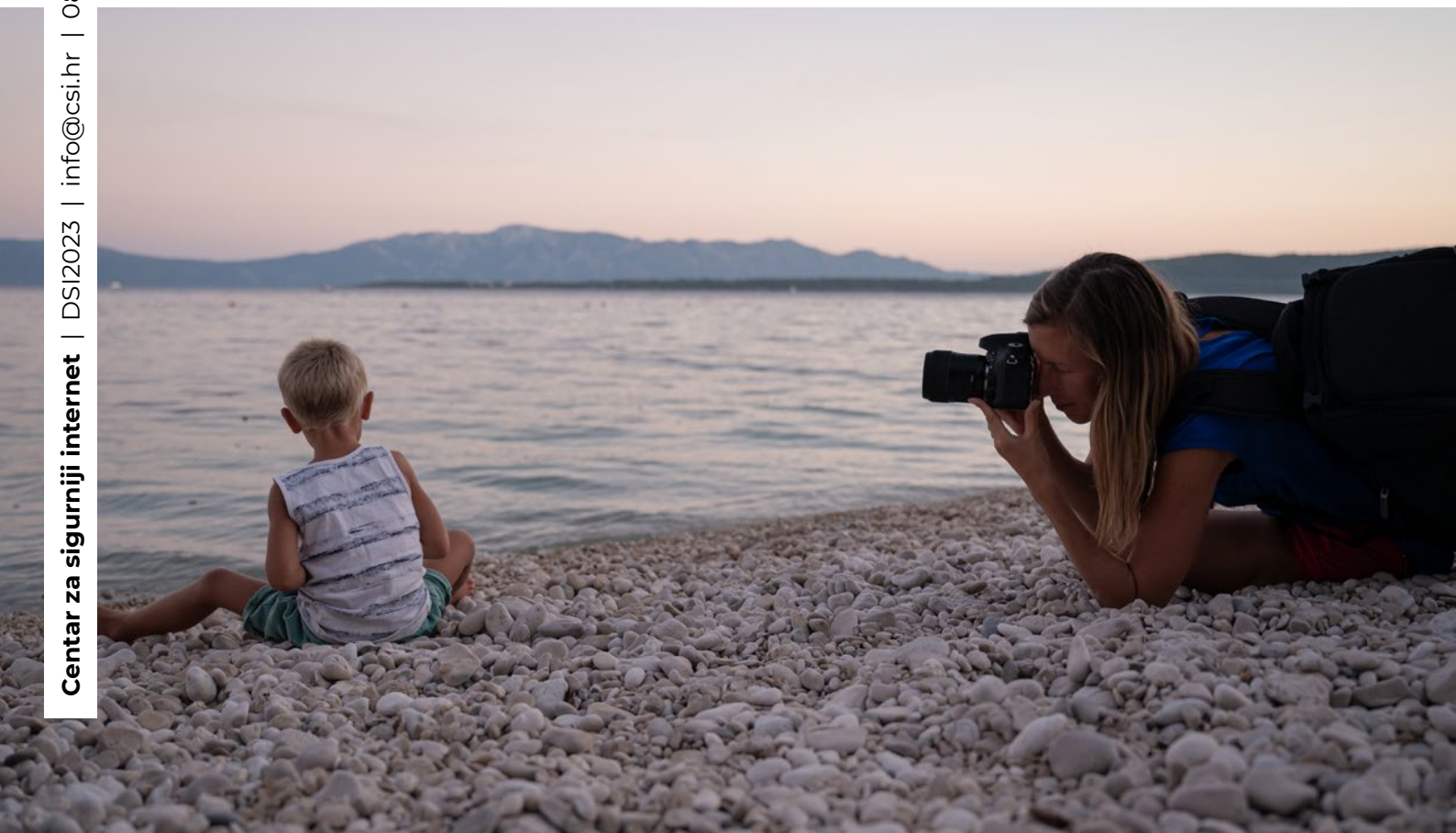
DODATAK ZA RODITELJE

SHARENTING

Pojam koji se odnosi na situacija kada roditelji ili članovi obitelji pretjerano objavljuju i dijele fotografije i podatke o djeci. Kombinacija je engleskih riječi ''sharing'' i ''parenting'' što bi se u duhu hrvatskog jezika moglo prevesti kao roditeljsko dijeljenje u digitalnom okruženju.

Pet pitanja koja si roditelji mogu postaviti prilikom objavljivanja takvog sadržaja:

1. Zašto to dijelim?
2. Biste li htjeli da netko takvu objavu podijeli o vama?
3. Može li ta objava osramotiti vaše dijete, sada ili u budućnosti?
4. Postoji li netko na ovom planetu tko ne bi trebao vidjeti to o vašem djetetu, bilo sada ili u budućnosti?
5. Je li to nešto što biste vi htjeli da bude dio digitalnog otiska vašeg djeteta?



GROOMING

Proces u kojemu se potencijalni seksualni zlostavljač sprijateljuje s djetetom te zadobiva njegovo povjerenje kako bi ga pokušao uključiti u (seksualne) zlostavljačke aktivnosti.

ZAŠTITITE SE OD GROOMINGA:

- Razgovarajte s djetetom o razlici između online i offline prijatelja – važno je naglasiti da koliko god se dragima i pristupačnima čine novi online prijatelji i dalje se radi o nepoznatoj osobi.
- Prepoznajte znakove – predlaganje offline upoznavanja, traženje osobnih informacija, traženje slika ili videozapisa djeteta, traženje djeteta da čuva tajnu.
- Saznajte gdje se nalaze gumbi za blokiranje i prijavu – društvene mreže, aplikacije, igrice i ostale web stranice nude opciju prijave ili blokiranja drugih korisnika.
- Uvjerite se da dijete zna da mu stojite na raspolaganju – djeca će često u strahu od reakcije roditelja prešutjeti nešto što smatraju osjetljivim ili uznemirujućim i to će ih spriječiti da potraže pomoć.
- Saznajte gdje možete potražiti dodatnu pomoć i podršku – na web stranicama Centra za nestalu i zlostavljanu djecu te na stranicama Centra za sigurniji internet možete pronaći sve potrebne kontakte i informacije kako bi dobili podršku u potencijalno ugrožavajućoj situaciji)

SEXTORTION

Sextortion je pojam koji dolazi od spajanja dvije riječi – sex i extortion – što bi u prijevodu značilo iznuda ili ucjena na temelju seksualnog sadržaja. Napadači od žrtava traže razne usluge seksualne prirode, novac ili druge usluge pod ucjenom da će objaviti intiman ili seksualno eksplicitan sadržaj žrtve. To se često odnosi na fotografije ili videa na kojima se nalazi žrtva – koje su u nekom trenutku počinitelju poslali same ili je takav materijal proizveden korištenjem raznih digitalnih alata (deepfake).

KAKO NAPADAČI DOLAZE DO SADRŽAJA?

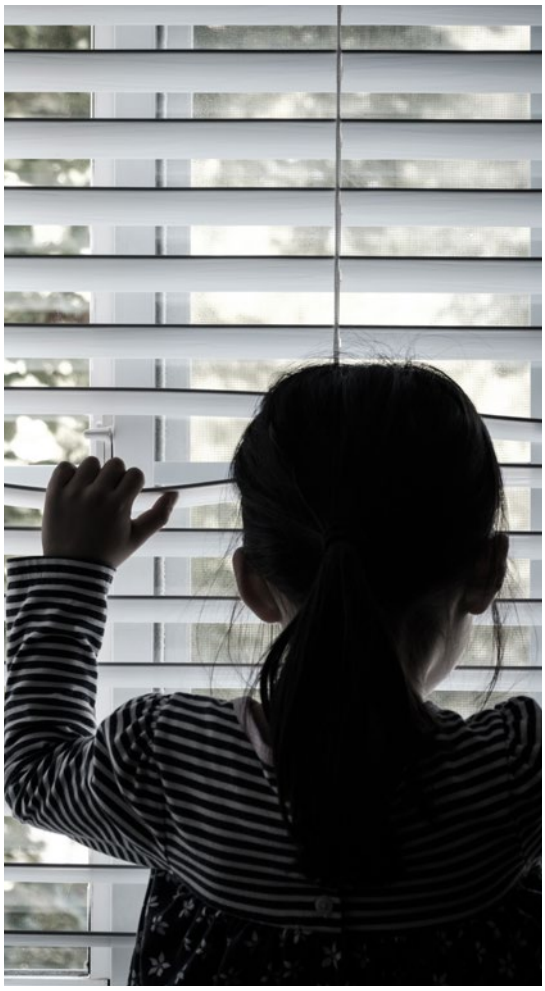
- uz pristanak žrtve koji je dobiven kroz izgradnju odnosa povjerenja kroz manipulaciju
- lažnim predstavljanjem
- potajnim snimanjem i/ili fotografiranjem bez pristanka žrtve
- hakiranjem korisničkih računa ili digitalnih uređaja žrtve.

KAKO SE ZAŠTITITI:

- nemojte slati intimne slike iz kojih se jasno može iščitati da ste to vi,
- nemojte slati slike na kojima se vidi vaše lice,
- nemojte slati slike na kojima se vide vaša prepoznatljiva obilježja poput tetovaža ili okruženje koje se jasno može prepoznati kao vaše.

CSAM

CSAM je kratica koja označava Child Sexual Abuse Material, odnosno materijal seksualnog zlostavljanja i iskorištavanja djece. Takav materijal može se pojaviti u bilo kojem obliku, a najčešće kao fotografije i videi. CSAM se često pogrešno naziva dječjom pornografijom, no djeca nikada ne mogu dati pristanak za kreiranje takvog sadržaja zbog čega je jedini ispravan naziv ''Materijal seksualnog zlostavljanja i iskorištavanja djece''.



KAKO UTJECATI NA SUZBIJANJE CSAM-A

- Ako se susretnete s ovakvim sadržajem prijavite ga bez odgode
- Ako sumnjate da je netko u životnoj opasnosti, odmah se obratite institucijama
- Takav sadržaj prijavite na csi.hr/hotline/
- Napravite sve u vašoj moći kako bi takav sadržaj u što kraćem vremenu bio uklonjen s interneta

ONLINE SEKSUALNO UZNEMIRAVANJE

Seksualno uznemiravanje na internetu definira se kao neželjeno seksualno ponašanje na bilo kojoj digitalnoj platformi i prepoznato je kao oblik seksualnog nasija. Ono uključuje širok raspon ponašanja koja koriste digitalni sadržaj i javlja se na raznim platformama, privatnim ili javnim.

SEKSUALNO UZNEMIRAVANJE NA INTERNETU UKLJUČUJE:

- Nesporazumno dijeljenje intimnih slika ili videa
- Iskorištavanje, prisilu i prijetnje
- Seksualizirano vršnjačko nasilje
- Neželjenu seksualizaciju

SEXTING

Sexting je ponašanje koje uključuje slanje, primanje i/ili prosljeđivanje eksplicitnog seksualnog sadržaja - fotografija, videa ili video poziva putem mobitela, računala ili bilo kojeg digitalnog uređaja. Kombinacija je engleskih pojmova ‘’sex’’ i ‘’texting’’ što se u doslovnom prijevodu može prevesti kao slanje seksualnih poruka.

Budući da danas djeca i mladi sve više koriste digitalne uređaje i vrijeme provode na društvenim mrežama, razmjenjuju poruke putem različitih aplikacija za komunikaciju, rizik od izloženosti sekstingu ili eksplicitnom sadržaju je povećan.

Kako bi se smanjilo primanje neprimjerenog sadržaja svakako preporučujemo da djeca koriste samo privatne korisničke račune na društvenim mrežama.