MODUL OBUKE ZA TRENERE NAMIJENJEN PROFESIONALCIMA NA "PRVOJ LINIJI" ZAŠTITE DJECE OD SEKSUALNOG ISKORIŠĆAVANJA I ZLOSTAVLJANJA NA INTERNETU

Projekta Savjeta Evrope za zaustavljanje seksualnog i skorišćavanja i zlostavljanja djece na internetu@Europe Plus

Gradimo Evropu za djecu i sa djecom

www.coe.int/children

Safe Online

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MODUL OBUKE ZA TRENERE NAMIJENJEN PROFESIONALCIMA NA "PRVOJ LINIJI" ZAŠTITE DJECE OD SEKSUALNOG ISKORIŠĆAVANJA I ZLOSTAVLJANJA NA INTERNETU

Projekta Savjeta Evrope za zaustavljanje seksualnog i skorišćavanja i zlostavljanja djece na internetu@Europe Plus

Autori:
David Wright i Bojana Miletić

Recenzija:
Hélène Paillard

Savjet Evrope

Naslov u originalu: Training of Trainers Module for Frontline Professionals on Safeguarding Children from Online Child Sexual Exploitation and Abuse

Mišljenja izražena u ovom radu odgovornost su autora i ne moraju nužno odražavati zvaničnu politiku Savjeta Evrope ili Safe Online.

Savjet Evrope sa zahvalnošću priznaje finansijsku podršku koju je za ovaj projekat obezbijedio Safe Online.

Safe Online je jedini globalni investicioni okvir posvećen zaštiti djece u digitalnom svijetu. Kroz ulaganje u inovacije i povezivanje ključnih aktera, Safe Online pomaže u oblikovanju digitalnog svijeta koji je siguran i osnažujuć za svu djecu i mlade svuda u sijvijetu.

Saznajte više na https://safeonline.global/.

Sva ostala korespondencija u vezi sa ovim dokumentom treba biti upućena Generalnoj direkciji za demokratiju i dostojanstvo čovjeka, Savjet Evrope, F-67075 Strazbur Sedeks.

Elektronska pošta: children@coe.int

Fotografija na naslovnoj strani: © Shutterstock.

Naslovna strana, pripema i ilustracije: Radna Soba

Sadržaj

Ciljevi obuke

Primarni cilj Programa obuke trenera o bezbjednosti na internetu (*Online Safety Train the Trainer Program, eng.*) je da osnaži odabranu grupu predavača/trenera u Gruziji, Republici Moldaviji i Crnoj Gori, sa neophodnim vještinama, znanjem i resursima kako bi djelotvorno zaštitili djecu od rizika na internetu. Ovi treneri će, zauzvrat, prenositi znanja sa obuke na druge profesionalce u svojim zemljama, stvarajući povratni efekat koji pojačava opseg i uticaj Programa.

Specifični ciljevi

1. **Povećati svijest i razumijevanje sigurnosti na internetu**: Učesnici će razviti duboko razumijevanje različitih rizika povezanih sa korišćenjem tehnologije od strane djece, sa fokusom na seksualno iskorišćavanje i zlostavljanje djece na internetu. Ovo uključuje ne samo razumijevanje različitih vrsta prijetnji na internetu, već i prepoznavanje psiholoških i društvenih faktora koji pogoršavaju ove rizike.
2. **Obučiti trenere/predavače praktičnim vještinama**: Program je osmišljen tako da pruža trenerima praktične vještine za identifikaciju, reagovanje i ublažavanje bezbjednosnih rizika na internetu. Navedeno uključuje učenje o najnovijim alatima, strategijama i tehnologijama, koje se mogu koristiti za zaštitu djece na internetu.
3. **Podsticati kritičko razmišljanje i rješavanje problema**: Kroz vježbe i diskusije zasnovane na scenarijima, učesnici će unaprijediti svoje kritičko razmišljanje i sposobnosti rješavanja problema. Učesnici će savladati primjenu teorijskog znanja na praktične situacije, čineći ih djelotvornijim u kontekstu stvarnog svijeta.
4. **Promovisati najbolje prakse i razvoj politika**: Učesnici će istraživati i dijeliti najbolje prakse u vezi sa bezbjednošću na internetu, pomažući u uspostavljanju okvira učinkovitih strategija i politika, koje se mogu primijeniti u njihovim vlastitim organizacijama i zajednicama.
5. **Izgraditi kapacitet za kontinuirano učenje i prilagođavanje**: Digitalno okruženje se konstantno razvija, a u skladu sa tim i rizici. Program ima za cilj da usadi način razmišljanja o kontinuiranom učenju i prilagođavanju, osiguravajući da predavači/treneri ostanu u toku sa najnovijim dostignućima u oblasti bezbjednosti na internetu.
6. **Olakšati učenje umrežavanjem i uz saradnju**: Okupljanjem profesionalaca iz različitih sektora i zemalja, Program podstiče okruženje za učenje kroz saradnju. Učesnici će imati priliku da se umreže, razmjenjuju iskustva i uče jedni od drugih, izgrađujući zajednicu sa praksom koja se proteže izvan same obuke.
7. **Osnažiti trenere/edukatore da prenose znanja**: Konačno, Program ima za cilj da omogući predavačima/trenerima da steknu veće samopouzdanje i sposobnost da svoje znanje i vještine prenesu drugim profesionalcima u njihovim zemljama. Ovaj efekat umnožavanja osigurava širi i održiviji uticaj, doseže do šire ciljne grupe i stvara sigurnije internet okruženje za djecu.

Ishodi

Na kraju dvodnevne obuke, učesnici će:

- Steći sveobuhvatno razumijevanje trenutnog okruženja bezbjednosti na internetu, uključujući nove tehnologije i s tim povezane rizike.
- Usvojiti vještine u identifikovanju i rješavanju specifičnih problema bezbjednosti na internetu u vezi sa seksualnim iskorišćavanjem i zlostavljanjem djece na internetu, ali takođe imati i širu svijest o srodnim pitanjima, kao što su zlostavljanje putem interneta, dezinformacije, bezbjednost uređaja i ubjedljiv dizajn u tehnologiji.
- Posjedovati praktične strategije i alate za sprovođenje učinkovitih mjera bezbjednosti na internetu u okviru svojih organizacija i zajednica.
- Biti u stanju uključiti i obrazovati roditelje o upravljanju digitalnim životima svoje djece, promovisanju zdrave upotrebe tehnologije i zaštiti privatnosti.
- Uspostaviti veze sa drugim profesionalcima, stvarajući mrežu za podršku za stalnu saradnju i razmjenu znanja.
- Biti spremni da pruže dalju obuku kolegama i drugim zainteresovanim stranama, čime se proširuje domet i uticaj Programa.

Program Online Safety Train the Trainer Program je sveobuhvatna inicijativa, koja ima za cilj da stvori sigurnije digitalno okruženje za djecu, osnaživanjem onih koji su na "prvim linijama" zaštite djece.

Struktura obuke

Dvodnevni program je strukturisan tako da izgradi razumijevanje, istraži specifična pitanja bezbjednosti na internetu i pruži praktične strategije za primjenu.

Dan 1: Okruženje i izazovi

Obuka počinje predstavljanjem, uspostavljanjem atmosfere saradnje i stvaranjem osjećaja zajedništva među učesnicima. Nakon toga slijedi sesija o promjenama tehnologija, gdje edukatori/treneri podučavaju o brzoj evoluciji tehnologije i njenim implikacijama na djecu, uključujući mogućnosti i rizike.

Zatim, sveobuhvatna rasprava o tome šta je bezbjednost na internetu pruža učesnicima razumijevanje različitih rizika povezanih sa korišćenjem tehnologije od strane djece, fokusirajući se na Sadržaj, Kontakt, Ponašanje i Ugovor. Ovo osnovno znanje je ključno za identifikaciju i ublažavanje rizika.

Nakon pauze, fokus se prebacuje na specifična pitanja bezbjednosti na internetu/zaštiti djece. Učesnici istražuju šire aspekte koji se odnose na seksualno iskorišćavanje i zlostavljanje djece na internetu i način na koji oni mogu biti međusobno povezani i uključuje psihološki uticaj uvjerljivog dizajna u tehnologiji, izazove u vezi sa bezbjednošću uređaja i dezinformacijama, nasilje na internetu, štetni sadržaj i uticaj tehnologije, te pritisak vršnjaka na dobrobit djece. Sesija se zatim fokusira na seksualno iskorišćavanje i zlostavljanje djece putem interneta, uključujući pregled konkretnih prijetnji i štete.

Pregled nacionalnih i međunarodnih akademskih istraživanja o bezbjednosti i na internetu pruža bazu dokaza koja podržava strategije i prakse o kojima se raspravlja. Slijede praktične vježbe koje koriste scenarije, pomažući učesnicima da svoje učenje primijene na situacije iz stvarnog života.

Dan završava sesijom koja se odnosi na tehnologije budućnosti, gdje učesnici uče da predviđaju i pripremaju se za buduće izazove u zaštiti djece.

Dan 2: Strategije i upravljanje

Dan drugi počinje pregledom ključnih tačaka obrađenih prvog dana, čime se učenje osnažuje. Prva velika sesija se fokusira na Strategije bezbjednosti na internetu za vaspitače/nastavnike, socijalne radnike i doktore, istražujući organizacione strategije za stvaranje i održavanje bezbjednog internet okruženja za djecu.

Nakon toga, sesija o Bezbjednosnim strategijama na internetu za roditelje osposobljava učesnike za korišćenje praktičnih alata i resursa koji pomažu roditeljima da djelotvorno upravljaju digitalnim životima svoje djece. Teme uključuju upravljanje vremenom ispred ekrana, postavke privatnosti, modeliranje upotrebe zdrave tehnologije i kako se nositi sa pritiscima među vršnjacima.

Učesnici zatim razmjenjuju svoje postojeće prakse na sesiji o postojećim bezbjednosnim praksama na internetu, učeći iz razmjene međusobnih iskustava i identifikujući djelotvorne strategije. Važan element je predstavljanje specifičnih nacionalnih mehanizama prevencije, izvještavanja i upućivanja.

Zatim, učesnici su sprovedeni kroz sistem raznih učinkovitih resursa za bezbjednost na internetu, koji im daju vrijedne alatke za podršku njihovim stalnim naporima. Obuka se završava rezimirajućom sesijom na kojoj se pregleda cijeli sadržaj, koji je pokriven obukom i razmatraju sva preostala pitanja.

Učesnici obuke će imati koristi kroz doprinose od kombinacije širokih aspekata međunarodnih stručnjaka, dopunjenih lokalnim kontekstom od strane domaćih stručnjaka.

Do kraja Programa, učesnici će steći sveobuhvatno razumijevanje o bezbjednosti na internetu i samopouzdanje da ovo znanje učinkovito prenesu u svoje zemlje. Ovaj strukturisani pristup osigurava da predavači/treneri budu dobro pripremljeni da ostvare značajan uticaj na zaštitu djece u digitalnom svijetu.

Plan obuke / Agenda

DAN 1 – OKRUŽENJE I IZAZOVI

Uvodno predstavljanje (30 minuta)

Uvod u obuku i ciljeve, predstavljanje učesnika/delegata i trenera.

Tehnologije koje se mijenjaju (60 minuta)

Tehnologija se mijenja nezapamćenim brzinom; koje su to tehnologije u nastajanju i mogućnosti koje one nude djeci

Šta je bezbjednost na internetu? (60 minuta)

Opšta diskusija o brojnim rizicima koje tehnologija predstavlja za djecu, preciznije "4C" (Sadržaj, Kontakt, Ponašanje i Ugovor - *Content, Contact, Conduct and Contract,* eng.)

Pauza za ručak

Specifična bezbjednost na internetu / pitanja koja se odnose na zaštitu djece (120 minuta)

Prilika da se dublje istraži i diskutuje o širim bezbjednosnim rizicima na internetu i o tome kako se oni mogu odnositi na seksualno iskorišćavanje i zlostavljanje djece na internetu, a posebno na.

- **Zdravlje i dobrobit**: Tehnologija i usluge su dizajnirane da ubijede i prisile korisnike da nastave da je koriste i da se vraćaju upotrebi tehnologije. Sesija će istražiti primjere ubjedljivog dizajna, uz osvrt na osnove psihologije, koji ne utiču samo na djecu, već i na roditelje, potencijalno odvlačeći njihovu pažnju od djece.
- **Računarsku bezbjednost**: Bezbjednost uređaja predstavlja sve veći izazov sa organizovanim kriminalom.
- **Dezinformacije i netačne informacije:** GenerativeAI (generativna vještačka inteligencija) predstavlja revoluciju u tehnologiji i kreiranju sadržaja, od kojih nisu svi tačni.
- **Zlostavljanje:** Istraživanje zlostavljanja na mreži i uticaja koji može imati.
- **Štetan sadržaj:** Pregled ranjivosti - Oni koji su izloženi najvećem riziku na internetu su takođe suočeni sa najvećim rizikom u fizičkom svijetu.
- **Uticaj**: Pregled uticaja koji tehnologija (*influenseri*) i okruženje (vršnjaci, braća i sestre) imaju na djecu i kako to utiče (slika tijela, FOMO itd.)

Fokusirana sesija o **seksualnom iskorišćavanju i zlostavljanju** djece na internetu, uz razmatranje:

- Štetnog seksualnog ponašanja na internetu,
- Materijala o seksualnom zlostavljanju djece, uključujući sintetički SIZDM (CSAM, eng.),
- Iznuda (novčana),
- Iskorišćavanje djece preko interneta,
- Procjena rizika od SIZDI-ja.

Dokazi iz istraživanja (30 minuta)

Literarni pregled objavljenih akademskih istraživanja (nacionalnih i međunarodnih) o bezbjednostii na internetu.

Scenariji (60 minuta)

Upotreba scenarija za vježbu u kojoj se diskutuje o implikacijama na djecu i kako odgovoriti.

Tehnologije budućnosti (60 minuta)

Sagledavajući buduće perspektive i tehnologije u nastajanju, posebno GenerativeAI (generativnu vještačku inteligenciju) i potencijalne rizike za djecu – šta učesnici treba da razmotre u budućnosti da bi ih zaštitili?

DAN 2 – STRATEGIJE I UPRAVLJANJE

Pregled dana 1 (30 minuta)

Kratki rezime, sa naglašavanjem aspekata razmatranih tokom dana prvog.

Strategije bezbjednosti na internetu za nastavnike/ predavače, socijalne radnike i doktore (90 minuta)

Detaljna diskusija o tome koje strategije, politike i alate treba da primijeni jedna organizacija da bi učinkovito zaštitila djecu na internetu, a posebno:

- Vlasništvo/autorstvo
- Izvještavanje
- Politike
- Usavršavanje osoblja
- Obrazovanje djece
- Bezbjednu tehnologiju
- Evaluaciju

Strategije bezbjednosti na internetu za roditelje (90 minuta)

Istraživanje strategija, alata i resursa dostupnih roditeljima da upravljaju korišćenjem tehnologije od strane članova njihovih porodica i stvaranjem ispravnog okruženja, a naročito:

- Da razumiju pristup i usluge – da utvrde koje uređaje posjeduju njihove porodice i koje usluge koriste njihova djeca, kako bi odredili obim pristupa internetu.
- Započeti razgovor – prijedlozi za pokretanje diskusija o tome kako ostati bezbjedan na internetu i ostvariti zdravu digitalnu ravnotežu.
- Alati za porodično dijeljenje i upravljanje izazovom koji donosi vrijeme provedeno ispred ekrana (“screen-time”) – rezime dostupnosti alata roditeljima za upravljanje i ograničavanje korišćenja uređaja i usluga od

strane njihove djece. Proširiti temu primjerima o tome kako upravljati vremenom provedenim ispred ekrana, posebno preko noći i u vrijeme obroka.

- Upravljanje pristupom – diskusija koja vodi od roditeljskih alata uključivanja fizičkih mjera za upravljanje pristupom, uključujući kada dati prvi mobilni telefon, povezivanje sa drugim roditeljima u borbi protiv vršnjačkog pritiska i sklapanja SMART porodičnih sporazuma.
- Upravljanje postavkama privatnosti – sažetak postavki privatnosti dostupnih na najpopularnijim servisima društvenih medija i kako im pristupiti.
- Digitalni uzor (kao roditelj) – svijest roditelja o korišćenju tehnologije i važnosti modeliranja zdrave upotrebe tehnologije.
- Upravljanje uticajem – kako pokrenuti zdrave diskusije sa djecom oko razumijevanja uticaja internetskih sadržaja (npr. na sliku tijela) i kako se nositi sa pritiskom vršnjaka.
- Zahtjevi za minimalnu starosnu dob – rezime najpopularnijih online usluga i s tim povezanih zahtjeva minimalne starosne dobi.

Pauza za ručak

Postojeća praksa bezbjednosti na internetu (60 minuta)

Mogućnost da se razmotre i podijele među učesnicima postojeće mjere i prakse bezbjednosti na internetu. Tokom sesije će se navesti primjeri dobre prakse.

Djelotvorni resursi za sigurnost na mreži (30 minuta)

Putokazi učibkovitih resursa za sigurnost na mreži.

Nacionalni okvir (60 minuta)

Pregled specifičnih nacionalnih mehanizama prevencije, prijavljivanja i upućivanja, uz postojeće protokole za svaku kategoriju profesionalaca u slučajevima nasilja nad djecom.

Rezime (30 minuta)

Pregled svih obuhvaćenih sadržaja i pružanje mogućnosti učesnicima obuke da postave pitanja radi pojašnjenja i konsolidacije razumijevanja.

Sadržaj obuke

1. PREZENTACIJA

Slajd 1

Primarni cilj Programa obuke trenera o bezbjednosti na internetu (*Online Safety Train the Trainer Program*, eng.) je osnažiti odabranu grupu trenera u Gruziji, Republici Moldaviji i Crnoj Gori neophodnim vještinama, znanjem i resursima kako bi učinkovito zaštitili djecu od rizika na internetu. Ovi predavači/treneri će, zauzvrat, prenositi saznanja sa obuke na druge profesionalce u svojim zemljama, stvarajući povratni efekat koji pojačava domet i uticaj Programa.

Specifični ciljevi

Povećati svijest i razumijevanje sigurnosti na internetu: Učesnici će razviti duboko razumijevanje različitih rizika povezanih sa korišćenjem tehnologije od strane djece, sa fokusom na seksualno iskorišćavanje i zlostavljanje djece na internetu. Ovo uključuje ne samo razumijevanje različitih vrsta prijetnji na internetu, već i prepoznavanje psiholoških i društvenih faktora koji pogoršavaju ove rizike.

Obučiti trenere/predavače praktičnim vještinama: Program je osmišljen tako da pruža trenerima praktične vještine za identifikaciju, reagovanje i ublažavanje bezbjednosnih rizika na internetu. Navedeno uključuje učenje o najnovijim alatima, strategijama i tehnologijama, koje se mogu koristiti za zaštitu djece na internetu.

Podsticati kritičko razmišljanje i rješavanje problema: Kroz vježbe i diskusije zasnovane na scenarijima, učesnici će unaprijediti svoje kritičko razmišljanje i sposobnosti rješavanja problema. Učesnici će savladati primjenu teorijskog znanja na praktične situacije, čineći ih djelotvornijim u kontekstu stvarnog svijeta.

Promovisati najbolje prakse i razvoj politika: Učesnici će istraživati i dijeliti najbolje prakse u vezi sa bezbjednošću na internetu, pomažući u uspostavljanju okvira učinkovitih strategija i politika, koje se mogu primijeniti u njihovim vlastitim organizacijama i zajednicama.

Izgraditi kapacitet za kontinuirano učenje i prilagođavanje: Digitalno okruženje se konstantno razvija, a u skladu sa tim i rizici. Program ima za cilj da usadi način razmišljanja o kontinuiranom učenju i prilagođavanju, osiguravajući da predavači/treneri ostanu u toku sa najnovijim dostignućima u oblasti bezbjednosti na internetu.

Olakšati učenje umrežavanjem i uz saradnju: Okupljanjem profesionalaca iz različitih sektora i zemalja, Program podstiče okruženje za učenje kroz saradnju. Učesnici će imati priliku da se umreže, razmjenjuju iskustva i uče jedni od drugih, izgrađujući zajednicu sa praksom koja se proteže izvan same obuke.

Osnažiti trenere/edukatore da prenose znanja: Konačno, Program ima za cilj da omogući predavačima/trenerima da steknu veće samopouzdanje i sposobnost da svoje znanje i vještine prenesu drugim profesionalcima u njihovim zemljama. Ovaj efekat umnožavanja osigurava širi i održiviji uticaj, doseže do šire ciljne grupe i stvara sigurnije internet okruženje za djecu.

Ishodi

Na kraju dvodnevne obuke, učesnici će:

- Steći sveobuhvatno razumijevanje trenutnog okruženja bezbjednosti na internetu, uključujući nove tehnologije i s tim povezane rizike.
- Usvojiti vještine u identifikovanju i rješavanju specifičnih problema bezbjednosti na internetu u vezi sa seksualnim iskorišćavanjem i zlostavljanjem djece na internetu, ali takođe imati i širu svijest o srodnim pitanjima, kao što su zlostavljanje putem interneta, dezinformacije, bezbjednost uređaja i ubjedljiv dizajn u tehnologiji.
- Posjedovati praktične strategije i alate za sprovođenje učinkovitih mjera bezbjednosti na internetu u okviru svojih organizacija i zajednica.
- Biti u stanju uključiti i obrazovati roditelje o upravljanju digitalnim životima svoje djece, promovisanju zdrave upotrebe tehnologije i zaštiti privatnosti.
- Uspostaviti veze sa drugim profesionalcima, stvarajući mrežu za podršku za stalnu saradnju i razmjenu znanja.
- Biti spremni da pruže dalju obuku kolegama i drugim zainteresovanim stranama, čime se proširuje domet i uticaj Programa.

Slajd 2 – Sadržaj (Dan 1)

Obuka će obuhvatiti slijedeće module:

1. **Uvodno predstavljanje:** Upoznavanje učesnika sa obukom i trenerima
2. **Tehnologije koje se mijenjaju:** Tehnologija se mijenja nezapamćenim brzinom; koje su to tehnologije u nastajanju i mogućnosti koje one nude djeci.
3. **Šta je bezbjednost na internetu?** Opšta diskusija o brojnim rizicima koje tehnologija predstavlja za djecu, preiznije "4C" (Sadržaj, Kontakt, Ponašanje i Ugovor - (*Content, Contact, Conduct and Contract*, eng.)
4. **Specifična bezbjednost na internetu / pitanja koja se odnose na zaštitu djece:** Prilika da se šire istraži i dublje razgovara o bezbjednosnim rizicima na internetu, kao i o tome kako se oni mogu odnositi na seksualno iskorišćavanje i zlostavljanje djece na internetu, a posebno na:
   - Zdravlje i dobrobit
   - Računarsku bezbjednost
   - Dezinformacije i netačne informacije
   - Zlostavljanje
   - Štetan sadržaj
   - Uticaj

   Fokusirana sesija o **seksualnom iskorišćavanju i zlostavljanju na internetu**, uz razmatranje:
   - Štetnog seksualnog ponašanja na internetu
   - Materijal o seksualnom zlostavljanju djece, uključujući sintetički SIZDM (CSAM, eng.)
   - Iznuda (novčana)
   - Iskorišćavanje djece na internetu
   - Procjena rizika od SIZDI
5. **Dokazi iz istraživanja:** Literarni pregled objavljenih akademskih istraživanja (nacionalnih i međunarodnih) o bezbjednosti na internetu.
6. **Scenariji:** Koriste se scenariji za vježbu u kojoj se raspravlja o implikacijama na djecu i kako odgovoriti na njih.
7. **Tehnologije budućnosti:** Gledajući u u budućnost i tehnologije u nastajanju, posebno *GenerativeAI* i potencijalne rizike za djecu – šta će učesnici morati da razmotre u budućnosti da bi ih zaštitili?

Kraj dana 1

Slajd 3 – Sadržaj (Dan 2)

Na početku dana 2, prvo ćemo rezimirati dan 1.

1. **Strategije bezbjednosti na internetu za nastavnike, socijalne radnike i doktore:** Detaljna diskusija o tome koje strategije, politike i alate treba da primijeni jedna organizacija da bi učinkovito zaštitila djecu na internetu, a posebno:
   - Vlasništvo/autorstvo
   - Izvještavanje
   - Politike
   - Usavršavanje osoblja
   - Obrazovanje djece
   - Bezbjednu tehnologiju
   - Evaluaciju
2. **Strategije bezbjednosti na internetu za roditelje:** Istraživanje strategija, alata i resursa dostupnih roditeljima da upravljaju korišćenjem tehnologije od strane članova njihovih porodica i stvaranjem ispravnog okruženja, a naročito:
   - Da razumiju pristup i usluge – da utvrde koje uređaje posjeduju njihove porodice i koje usluge koriste njihova djeca, kako bi odredili obim pristupa internetu.
   - Započeti razgovor – prijedlozi za pokretanje diskusija o tome kako ostati bezbjedan na internetu i ostvariti zdravu digitalnu ravnotežu.
   - Alati za porodično dijeljenje i upravljanje izazovom koji donosi vrijeme provedeno ispred ekrana ("*screentime*") – rezime dostupnosti alata roditeljima za upravljanje i ograničavanje korišćenja uređaja i usluga od strane njihove djece. Proširiti temu primjerima o tome kako upravljati vremenom provedenim ispred ekrana, posebno preko noći i u vrijeme obroka.
   - Upravljanje pristupom – diskusija koja vodi od roditeljskih alata uključivanja fizičkih mjera za upravljanje pristupom, uključujući kada dati prvi mobilni telefon, povezivanje sa drugim roditeljima u borbi protiv vršnjačkog pritiska i sklapanja SMART porodičnih sporazuma.
   - Upravljanje postavkama privatnosti – sažetak postavki privatnosti dostupnih na najpopularnijim servisima društvenih medija i kako im pristupiti.
   - Digitalni uzor (kao roditelj) – svijest roditelja o korišćenju tehnologije i važnosti modeliranja zdrave upotrebe tehnologije.
   - Upravljanje uticajem – kako pokrenuti zdrave diskusije sa djecom oko razumijevanja uticaja internetskih sadržaja (npr. na sliku tijela) i kako se nositi sa pritiskom vršnjaka.

   Zahtjevi za minimalnu starosnu dob – rezime najpopularnijih online usluga i s tim povezanih zahtjeva minimalne starosne dobi.
3. **Postojeća praksa bezbjednosti na internetu:** Mogućnost da se razmotre i podijele među učesnicima vaše postojeće mjere i prakse bezbjednosti na internetu. Tokom sesije će se navesti primjeri dobrih praksi.
4. **Nacionalni okvir:** Pregled specifičnih nacionalnih mehanizama prevencije, prijavljivanja i upućivanja, uz postojeće protokole za svaku kategoriju profesionalaca u slučajevima nasilja nad djecom.
5. **Resursi za bezbjednost na internetu:** Označavanje djelotvornih resursa za bezbjednost na internetu.
6. **Rezime:** Pregled svih obuhvaćenih sadržaja i pružanje mogućnosti učesnicima da postave pitanja radi pojašnjenja i konsolidacije razumijevanja.

2. UVOD

Slajd 4

Svi u prostoriji predstavljaju sebe i svoje organizacije.

Slajd 5

Predstavljanje trenera.

Slajd 6

Predstavljanje organizacije/centra nacionalnog trenera.

Slajd 7 – Zabilješke trenera

SIZD(I) je osjetljiva tema i treba upamtiti značaj stvaranja prijateljske i neformalne atmosfere, kako bi se ljudi osjećali ugodno tokom razgovora o njoj.

Treneri bi trebalo da se unaprijed dogovore o proceduri u slučaju da se učesnik obuke javi kao žrtva SIZD-a.

3. TEHNOLOGIJE KOJE SE MIJENJAJU

Slajd 8

Tehnologije koje se mijenjaju - Tehnologija se mijenja nezapamćenim brzinom; koje su to tehnologije u nastajanju i mogućnosti koje one nude djeci.

Slajd 9 – Razmjere prisustva tehnologije u domovima

Uvod: Na ovom slajdu istražujemo rastuću prisutnost povezanih tehnologija u našim domovima. Tradicionalno, mislimo na laptopove, tablete i mobilne telefone, ali u mnogim kućama se nalazi širok spektar pametnih uređaja. Ova diskusija ima za cilj da podstakne učesnike da razmisle o razmjerama prisutnosti tehnologije u njihovim domovima i njenom uticaju na privatnost i bezbjednost**.**

Pregled slajda:

Cilj: Istaknuti raznolikost povezanih uređaja u savremenim domovima i razgovarati o njihovom uticaju na porodični život i bezbjednost**.**

Ključne tačke:

- **Tradicionalni uređaji:**
  - **Laptopovi, tableti i mobilni telefoni**: Razgovarajte o širokoj upotrebi ovih tradicionalnih uređaja u svakodnevnom životu za komunikaciju, posao i zabavu.
- **Povezana kuhinja:**
  - Pametni aparati: Navesti pametne frižidere koji mogu pratiti zalihe i predlagati recepte, pametne pećnice koje se mogu kontrolisati na daljinu i pametne sijalice koje prilagođavaju osvjetljenje.
  - Centralno grijanje: Istaknuti pametne termostate koji uče korisničke preferencije i mogu se kontrolisati putem aplikacija na pametnim telefonima.
- **Tehnologija u dnevnom boravku:**
  - Pametni televizori: Razgovarati o tome kako pametni televizori nude usluge sitrimovanja, pretrage interneta i integraciju sa drugim pametnim kućnim uređajima.
  - Pametni zvučnici: Objasniti ulogu pametnih zvučnika kao što su *Amazon Echo* i *Google Hom*e u kontrolisanju drugih uređaja, puštanju muzike i odgovaranju na upite.
- **Dječje sobe:**
  - **Konzole za igre:** Spomenuti popularne konzole za igre, poput *PlayStationa* i *Xboxa,* koje nude ne samo igre (“*gaming*”, eng.) već i usluge *strimovanja* i *online* interakciju.
  - **Obrazovni uređaji:** Istaknuti pametne igračke i uređaje, koji se koriste u obrazovne svrhe povezane su na internet radi ažuriranja sadržaja i interakcije.

- **Kancelarija u kući:**
  - **Kompjuteri i štampači**: Razgovarati o suštinskoj ulozi računara i štampača u postavci kancelarije u kući.
  - **Oprema za umrežavanje**: Navesti rutere i modeme koji su ključni za internet konekciju i često uključuju pametne funkcije.
- ***Cloud*:**
  - **Skladištenje podataka**: Objasniti koliko domaćinstava koristi usluge *Cloud*-a za skladištenje dokumenata, fotografija i drugih važnih fajlova. Istaknuti pogodnost i potencijalnu zabrinutost za privatnost skladištenja u *Cloud*-u.

Koraci za akciju:

- **Interaktivna vježba:** Zamoliti učesnike da nabroje sve povezane uređaje u svojim domovima, po prostorijama. Potencijalno obezbijediti obrazac ili radni list za ovu aktivnost**.**
- **Pitanja za diskusiju:**
  - **"**Koje su neke od prednosti i izazova u odnosu na više povezanih uređaja u kući?"
  - "Kako obezbjeđujete sigurnost ovih uređaja?"
- **Dijeljenje resursa:** Obezbijediti linkove do izvora o obezbjeđivanju pametnih kućnih uređaja i upravljanju postavkama privatnosti**.**

Diskusija:

- **Lična iskustva:** Pozvati učesnike da podijele svoja iskustva sa pametnim kućnim uređajima. Koje prednosti su zapazili? Sa kojim izazovima su se suočili?
- **Bezbjednosne mjere:** Razmotriti uobičajene bezbjednosne mjere, kao što su promjena zadatih lozinki, održavanje softvera ažuriranim i korišćenje dvofaktorske autentifikacije.

Zaključak: Sve veći broj povezanih uređaja u našim domovima nudi mnoge pogodnosti, ali takođe predstavlja izazove za privatnost i sigurnost. Razumijevanjem razmjera tehnologije u našim domovima, možemo preduzeti korake da zaštitimo svoje porodice i lične podatke**.**

Slajd 10 – Nacionalni podaci o korišćenju tehnologije od strane djece

Uvod: U ovom odjeljku ćemo ispitati nacionalne podatke o upotrebi i iskustvu upotrebe tehnologija kod djece. Navedeni primjer je iz *Ofcoma*, koji nudi vrijedne uvide u digitalne navike i bezbjednosne zabrinutosti kod djece u UK. Ovi podaci služe kao model za razumijevanje sličnih trendova u drugim regijama i mogu se dopuniti ili zamijeniti konkretnijim nacionalnim dokazima gdje su dostupni.

Pregled slajda:

- **Cilj:** Istaknuti važnost nacionalnih podataka u razumijevanju korišćenja tehnologije i iskustava djece i podstaći korišćenje lokalnih podataka tamo gdje su dostupni.

Ključne tačke:

- **Svrha nacionalnih podataka:**
  - **Razumijevanje trendova:** Nacionalni podaci pomažu u identifikaciji trendova u načinu na koji djeca koriste tehnologiju, uključujući obrasce korišćenja i popularne platforme.
  - **Kreiranje politika:** Ovi podaci informišu kreatore politika, edukatore i roditelje, pomažući u razvoju učinkovitih strategija za digitalnu sigurnost i obrazovanje.
  - **Komparativna analiza:** Omogućava poređenje između različitih regiona, pomažući da se identifikuju jedinstveni izazovi i najbolje prakse**.**
- **Primjer: *Ofcom* podaci (UK):**
  - **Statistika upotrebe**: Razgovarajte o procentu djece koja koriste različite vrste uređaja i učestalosti njihove upotrebe.

- **Popularnost platforme**: Istaknite koje su platforme (npr. društvene mreže, igre) najpopularnije među djecom.
- **Bezbjednosna pitanja**: Podijelite statistiku o pitanjima kao što su zlostavljanje putem interneta, zabrinutost za privatnost i izloženost neprikladnom sadržaju.

- **Implikacije podataka:**
  - **Roditeljska svijest**: Naglasite potrebu da roditelji budu svjesni digitalnih aktivnosti svoje djece i platformi koje koriste.
  - **Obrazovne inicijative:** Istaknite kako škole mogu koristiti ove podatke za integraciju digitalne pismenosti i bezbjednosti u nastavni plan i program.
  - **Razvoj politike**: Razgovarajte o tome kako kreatori politika mogu primijeniti ove podatke za stvaranje sigurnijeg online okruženja za djecu.
- **Podsticanje korišćenja lokalnih podataka**:
  - **Relevantnost:** Naglasite važnost korišćenja lokalnih podataka kako biste osigurali relevantnost i primjenjivost u specifičnom kontekstu ciljne grupe.
  - **Pristupačnost:** Dajte savjete o tome gdje pronaći lokalne podatke, kao što su vladini izvještaji, akademske studije i ankete lokalnih organizacija.
  - **Prilagodljivost:** Predložite načine za prilagođavanje nalaza iz nacionalnih podataka lokalnom okruženju, uzimajući u obzir kulturne i regionalne razlike.

Koraci djelovanja:

- **Interaktivna vježba**: Zamolite učesnike da podijele sve nacionalne podatke ili izvještaje za koje znaju iz svojih zemalja. Podstaknite raspravu o tome kako se ovi podaci mogu iskoristiti u njihovoj profesionalnoj praksi.
- **Pitanja za diskusiju:**
  - "Koji su neki od ključnih nalaza iz nacionalnih podataka o korišćenju tehnologije od strane djece u vašoj zemlji?"
  - **"**Kako možemo koristiti ove nalaze za poboljšanje digitalne bezbjednosti i obrazovanje u našim lokalnim zajednicama?"
- **Dijeljenje resursa**: Omogućite linkove do relevantnih nacionalnih izvještaja i baza podataka gdje učesnici mogu pronaći dodatne informacije.

Diskusija:

- **Lična iskustva** Pozovite učesnike da podijele svoja iskustva sa nacionalnim podacima. Kako im je to pomoglo u njihovim ulogama? Koje praznine vide u dostupnim podacima?
- **Korišćenje podataka:** Razgovarajte o praktičnim načinima korišćenja ovih podataka za informisanje o nastavnoj praksi, roditeljskom usmjeravanju i kreiranju politika.

Zaključak: Nacionalni podaci o korišćenju tehnologije od strane dece su ključni za razumijevanje trendova, identifikaciju bezbjednosnih problema i informisanje o djelotvornim politikama i praksi. Primjenjujući ove podatke, možemo bolje podržati bezbjednu i odgovornu upotrebu digitalnih tehnologija koje koriste djeca.

Slide 11 – Dokazi iz nacionalnog okruženja

U Crnoj Gori trenutno ne postoji tijelo koje kontinuirano prati ponašanje građana i posebno ponašanje djece na internetu. Međutim, proteklih godina, formirana su odgovarajuća tijela koja se bave bezbjednošću na internetu.

U Crnoj Gori postoji nekoliko ključnih tijela i organizacija koje se bave sajber bezbjednošću, uključujući i pitanja vezana za zaštitu djece u digitalnom okruženju:

1. **Direkcija za informacionu bezbjednost (Vladin CIRT)** - Ova direkcija funkcioniše kao Vladin sigurnosni operativni centar (G-SOC) i bavi se monitorisanjem sajber ekosistema, rješavanjem incidenata i edukacijom o računarskoj bezbjednosti. Planirano je osnivanje Agencije za sajber bezbjednost koja bi uključila Nacionalni CIRT za zaštitu kritične informatičke infrastrukture.

2. **Ministarstvo javne uprave, digitalnog društva i medija** - Koordinira sajber bezbjednosne politike i aktivnosti, uključujući izradu strategija za unaprjeđenje digitalne sigurnosti.
3. **Direkcija za zaštitu tajnih podataka i Agencija za nacionalnu bezbjednost** - Aktivno doprinose razvoju i sprovođenju strategija sajber bezbjednosti u zemlji.
4. ***Women 4 Cyber Montene*gro** - Ova organizacija promoviše edukaciju i svijest o sajber bezbjednosti, s posebnim fokusom na zaštitu djece i žena u digitalnom prostoru.
5. **Ministarstvo prosvjete, nauke, kulture i sporta** - Uključeno je u edukativne inicijative koje podižu svijest o digitalnoj pismenosti i bezbjednosti među djecom i mladima.
6. **Regionalne inicijative** - Crna Gora aktivno učestvuje u međunarodnim projektima i vježbama poput *ITU Cyberdrill*, gdje se razmjenjuju najbolji globalni pristupi sajber sigurnosti.
7. **Zaštitnik ljudskih prava i sloboda Crne Gore** (Ombudsman) je od ključne važnosti za zaštitu prava djece, uključujući i njihovu sigurnost u digitalnom okruženju.

4. ŠTA JE BEZBJEDNOST NA INTERNETU?

Slajd 12 – Odjeljak o bezbjednosti na internetu

Opšta diskusija o nizu rizika koje tehnologija predstavlja za djecu, posebno "4 C" (sadržaj, kontakt, ponašanje i ugovor - (*Content, Contact, Conduct and Contract*, eng.).

Slajd 13 – Diskusija o tome šta je bezbjednost na internetu

Podstaknite učesnike da iznesu svoje mišljenje o tome šta smatraju da je bezbjednost na internetu – koja su to pitanja koja opažaju i doživljavaju.

Slide 14 - Rizici i prijetnje sa kojima se djeca suočavaju na internetu

Uvod

Na ovom slajdu istražujemo kategorizaciju rizika i prijetnji sa kojima se djeca suočavaju na internetu. Okvir "4 C" profesorice Sonia Livingstone[1] je djelotvoran model za razumijevanje ovih složenih i različitih opasnosti.

Pregled slajda

- Pregled "4 C"
  - "4 C" označava sadržaj, kontakt, ponašanje i ugovor. Ove kategorije obuhvataju niz rizika sa kojima se djeca suočavaju na internetu. Svaka kategorija ističe različite dimenzije potencijalne štete.
- **Rizici sadržaja:**
  - **Opis:** Rizici sadržaja uključuju izlaganje potencijalno štetnom materijalu.
  - **Primjeri:** Nasilne, krvave, eksplicitne, rasističke, ispunjene mržnjom ili ekstremističke informacije, kao i štetna ili ilegalna pornografija, seksualizacija kulture i opresivni normativi tjelesnog izgleda.
  - **Uticaj:** Oni mogu negativno uticati na djetetovo mentalno zdravlje, razvoj i pogled na svijet.
- **Rizici kontakta**
  - **Opis:** Rizici kontakta se odnose na štetne interakcije sa odraslima na internetu.
  - **Primjeri**: Uznemiravanje, proganjanje, ponašanje iz mržnje (netrpeljivost), neželjeni ili pretjerani nadzor, seksualno uznemiravanje, mamljenje u cilju vršenja krivičnih djela protiv polne slobode, seksualna ucjena i dijeljenje ili traženje materijala seksualnog zlostavljanja djeteta.
  - **Uticaj**: Takve interakcije mogu dovesti do psihološke i fizičke opasnosti, manipulacije i iskorišćavanja.

1 4 Cs of online risk: Short report & blog on updating the typology of online risks to include content, contact, conduct, contract risks – CO:RE Knowledge Base (core-evidence.eu)

- **Rizici ponašanja**
    - **Opis**: Rizici ponašanja vezani su za to kako se djeca ponašaju na internetu i kako ih takvo ponašanje može izložiti riziku.
    - **Primjeri**: Zlostavljanje, gruba ili neprijateljska komunikacija, vršnjačke aktivnosti kao što su trolovanje, isključivanje, javno sramoćenje i učešće u rizičnim izazovima. Zahtjevi za pravljenje seksualnog sadržaja koji sami generišu, seksualno uznemiravanje i seksualna ucjena.
    - **Uticaj**: Ovo može dovesti do odmazde, gubitka privatnosti ili fizičke i psihičke opasnosti.
- **Rizici ugovora**
    - **Opis**: Rizici ugovora se odnose na iskorišćavanje preko komercijalnih aktivnosti.
    - **Primjeri**: Krađa identiteta, prevara, krađa podataka putem lažnih poruka (*oblik internet prevare, phishin*g, eng.), obmana, hakovanje, ucjene, sigurnosni rizici, prodaja/kupovina SIZDIM-a, prenos uživo (*streaming*, eng.) i trgovina ljudima u cilju seksualne eksploatacije.
    - **Uticaj:** Djeca mogu pretrpjeti finansijske gubitke, neovlašćene naplate i kompromitaciju ličnih podataka. Kao dodatna napomena, trgovina djecom može rezultirati [teškim] traumama, PTSD-om (*postraumatski stresni poremećaj*), stigmatizacijom, diskriminacijom, izolacijom, reproduktivnim zdravstvenim problemima i sl.

Međusektorska pitanja: Dodatno, ovi rizici otvaraju međusektorska pitanja, uključujući kršenje privatnosti, rizike za fizičko i mentalno zdravlje, te nejednakosti i diskriminaciju. Oni naglašavaju rasprostranjenu prirodu rizika na internetu i naglašavaju potrebu za sveobuhvatnim zaštitnim mjerama.

Tačke za diskusiju – Pitanja za uključivanje ciljne grupe:

- Kako vidite da se ovi rizici manifestuju u vašem profesionalnom iskustvu?
- Koje strategije smatrate djelotvornim u ublažavanju ovih rizika za djecu?

Završne riječi

Razumijevanje okvira "4 C" pomaže nam da bolje zaštitimo djecu u digitalnom dobu. Ističe važnost budnosti i proaktivnih mjera kako bi se osigurala njihova sigurnost i dobrobit na internetu.

5. SPECIFIČNA PITANJA O BEZBJEDNOSTI/ PITANJA ZAŠTITE DJECE NA INTERNETU

Slajd 15

Prilika da se detaljnije istraži i razgovara o širim bezbjednosnim rizicima na internetu i kako se oni mogu odraziti na seksualno iskorišćavanje i zlostavljanje djece na internetu - Koja su to specifična pitanja zaštite djece?

Slajd 16 – Opšta pitanja koja utiču na bezbjednost djece na internetu

Pregled slajda:

- **Sadržaj:** Uvod u šest ključnih pitanja: zdravlje i dobrobit, računarska sigurnost, dezinformacije i netačne informacije, zlostavljanje, štetan sadržaj i uticaj.

Ključne tačke koje treba pokriti:

- **Uvid u opšta pitanja:**
  - Značaj razumijevanja različitih pitanja o bezbjednosti na internetu koja utiču na djecu.
  - Priroda međusobne povezanosti ovih pitanja zahtijeva sveobuhvatan pristup.
- **Zdravlje i dobrobit:** Tehnologija i usluge su kreirane na način da uvjere i privuku korisnike da neprekidno koriste i da se stalno vraćaju korišćenju tehnologija. Sesija će istražiti primjere ubjedljivog dizajna, dotičući se temeljne psihologije, koji ne utiču samo na djecu, već i na roditelje, potencijalno odvlačeći njihovu pažnju od njihove djece**.**
- **Računarska bezbjednost:** Bezbjednost uređaja je sve izazovnija sa organizovanim kriminalom.
- **Dezinformacije i netačne informacije:** Generativna vještačka inteligencija donosi revoluciju u tehnologiji i kreiranju sadržaja, ali takvi sadržaji nisu uvijek tačni.
- **Zlostavljanje**: Istraživanje zlostavljanja na internetu i kakav to može imati uticaj.
- **Štetan sadržaj**: Pregled ranjivosti- Ko je najviše ugrožen na internetu, a ko u fizičkom svijetu.
- **Uticaj:** Pregled uticaja koji tehnologija (*influenseri*) i okolina (vršnjaci, braća i sestre) imaju na djecu i kakve su posljedice (slika o svom tijelu, FOMO (*strah od propuštanja nečeg važnog - Fear of missing out, eng.*), itd.

Zatim ćemo imati fokusiranu sesiju o seksualnom iskorišćavanju I zlostavljanju djece na internetu:

- Važnost razumijevanja i odgovora na seksualno iskorišćavanje i zlostavljanje djece na internetu (SIZDI).
- Glavne teme koje će se obrađivati u sljedećoj sesiji:
  - Štetno seksualno ponašanje na internetu
  - Materijal o seksualnom zlostavljanju djece, uključujući sintetički SIZDM
  - Iznuda (novčana)

- Seksualno iskorišćavanje djece na internetu
- Procjena rizika od SIZDI-ja

Slajd 17 – Uticaj interneta

Pregled slajda:

- **Sadržaj:** Istraživanje načina na koji se na djecu vrši uticaj na internetu koristeći primjere i studije slučaja.

Ključne tačke za razmatranje:

- Uvod o uticaju preko interneta:
  - Značaj razumijevanja kako se na djecu utiče u digitalnom svijetu.
  - Različiti izvori uticaja uključujući društvene medije, *influensere*, vršnjake i samu tehnologiju.
- **Mehanizmi uticaja:**
  - Algoritmi i personalizovani sadržaj koji ciljaju na dječja interesovanja i ponašanja.
  - Uloga influensera na društvenim mrežama u oblikovanju dječjeg mišljenja, ponašanja i slike o sebi.
  - Uticaj vršnjaka preko društvenih mreža i interakcije na internetu.
- **Vrste uticaja:**
  - Pozitivan uticaj: obrazovni sadržaj, podrška zajednice.
  - Negativan uticaj: pitanja o slikama tijela, strahu od propuštanja nečeg važnog (*FOMO*, eng.) i pritisku vršnjaka.
- **Pitanja za diskusiju:**
  - Kako roditelji i edukatori mogu pomoći djeci da se nose sa uticajem na internetu.
  - Strategije za podsticanje kritičkog mišljenja i medijske pismenosti kod djece.
  - Važnost praćenja i postavljanja granica za aktivnosti na internetu.
- **Napomene o učešću:**
  - Podstaknite učesnike da podijele svoja zapažanja ili zabrinutosti o ponašanju djece na mreži.
  - Koristite primjere iz stvarnog života i studije slučaja da ilustrujete teze.
  - Odvojite vrijeme za pitanja i diskusije, kako biste produbili razumijevanje.

Slajd 18

Pustite video klip - Ovaj video otkriva da se često veoma vodi računa o tome kako uljepšati izgled na internetu, koji često nije istinit, niti realističan.

Slika tijela, kao primjer.

Problemi sa prikazivanjem tijela na internetu:

- **Izloženost idealizovanim slikama:** Platforme društvenih medija često prikazuju uređene, filtrirane i idealizovane slike standarda ljepote i tijela, što može stvoriti nerealna očekivanja**.**
- **Kultura poređenja**: Konstantno izlaganje ovim slikama dovodi do poređenja, čineći da se pojedinci, posebno mladi ljudi, osjećaju neodgovarajuće ili nezadovoljno vlastitim tijelom.
- **Pritisak vršnjaka:** Interakcije na mreži mogu uključivati komentare i "lajkove", koji pojačavaju značaj izgleda, čime se povećava pritisak za prilagođavanje ovim idealima.
- **Zlostavljanje na internetu**: Negativni komentari i osjećaj sramoćenja zbog sopstvenog tijela mogu pogoršati probleme sa slikama izgleda tijela i doprinijeti niskom samopoštovanju i problemima mentalnog zdravlja.

Efekti uticaja interneta:

- **Mentalno zdravlje:** Negativna slika o izgledu tijela pod uticajem sadržaja na internetu može dovesti do depresije, anksioznosti, poremećaja u ishrani i drugih problema sa mentalnim zdravljem.
- **Promjene u ponašanju**: Pojedinci mogu postati skloni nezdravom ponašanju, kao što su ekstremna dijeta ili pretjerano vježbanje, kako bi postigli percipirane idealne tjelesne standarde.
- **Sampoštovanje:** Česta poređenja i negativne povratne informacije mogu značajno smanjiti samopoštovanje i samovrednovanje.

Ukupan uticaj:

Uticaj interneta duboko se odražava na predstavu o izgledu tijela, promovišući nerealne standarde, njegujući kulturu poređenja, a ponekad i dovodeći do štetnog mentalnog zdravlja i ishoda ponašanja.

Slajd 19 – Zdravlje i dobrobit

Slajd 20 – Vrijeme provedeno na internetu

Pitanja za diskusiju:

- Koliko vremena djeca provode na internetu?
- Koliko vremena odrasli provode na internetu?
- Da li grupa provodi previše ili nedovoljno vremena na internetu?

Slajd 21 – Mentalno zdravlje i dobrobit - Ubjedljiv dizajn

Pregled slajda:

- **Sadržaj:** Istraživanje kako ubjedljiv dizajn u tehnologiji utiče na mentalno zdravlje i dobrobit, sa primjerima i interaktivnim pitanjima.

Ključne tačke za razmatranje:

- **Uvod u ubjedljiv dizajn:**
  - Definicija: Ubjedljiv dizajn podrazumijeva korišćenje psiholoških principa za uticaj na ponašanje korisnika.
  - Svrha: Kreirano da monopoliše vrijeme korisnika i drži ih angažovane sa uređajima i uslugama.
- **Interaktivna pitanja za animiranje učesnika:**
  - **Pitanje:** «Šta je prva stvar koju ste uradili ovog jutra kada ste se probudili? «
    - Vjerovatan odgovor: Provjeravao(la) vijesti, poruke, ili društvene mreže na mobilnom uređaju.
  - **Pitanje:** "Kada ste posljednji put provjerili svoj mobilni telefon?"
    - Naglasite učestalost i automatsku prirodu ovog ponašanja.
- **Objašnjenje tehnika ubjedljivog dizajna:**
  - **Mehanizam osvježavanja:**
    - Analogija: Poređenje sa kockanjem i slot mašinama.
    - Akcija: Povlačenje prstom preko ekrana radi ažuriranja dolazeće pošte ("*inbox*") ili medijskog striminga, slično je kao povlačenje ručice na slot mašini.
    - Efekat: Stvara očekivanje i prisiljava korisnike da provjeravaju dolazak novih informacija.
  - **Snapstreaks*:***
    - Definicija: Funkcija u *Snapchat-u (*trenutna komunikacija), gdje korisnici uzastopno šalju snimke naprijed-nazad, kako bi zadržali niz.
    - Uticaj: Podstiče svakodnevni angažman i redovnu interakciju, kako bi se izbjeglo prekidanje niza.
  - **Tri tačke (Indikatori kucanja):**

        - Opis: Pulsirajuće tačke ukazuju na to da neko odgovora na poruku.
        - Svrha: Zadržava korisnike u aplikaciji za poruke dok čekaju na odgovor.
        - Efektivnost: Povećava vrijeme provedeno u aplikaciji dok korisnici čekaju dolazeće poruke.
- **Uticaj na mentalno zdravlje i dobrobit:**
    - Produženo vrijeme provedeno pored ekrana može dovesti do:
        - Anksioznosti i stresa.
        - Poremećenog ritma spavanja.
        - Smanjiti socijalnu interakciju "licem u lice".
    - Kontinuirano bavljenje uređajima može skrenuti pažnju sa stvarnih životnih interakcija i odgovornosti.
- **Tačke za diskusiju:**
    - Kako korisnici mogu postati svjesniji ovih tehnika dizajna?
    - Koje strategije se mogu koristiti za smanjenje negativnog uticaja ubjedljivog dizajna?
    - Uloga roditelja i edukatora u pomaganju djeci da upravljaju vremenom provedenim ispred ekrana i steknu zdrave digitalne navike.

Napomene za učešće:

- Podstaći učesnike da podijele svoja iskustva sa elementima ubjedljivog dizajna.
- Koristiti primjere iz stvarnog života i predstaviti korišćenje mobilnog telefona.
- Odrediti vrijeme za pitanja i promišljanje kako bi se probudilo razumijevanje.

Slajd 22 – Računarska bezbjednost

Slajd 23 – Ukrštanje računarske bezbjednosti, bezbjednosti na internetu, zašitite i medijske pismenosti

Pregled slajda:

- **Sadržaj:** Diskusija o međusobnoj povezanosti računarske bezbjednosti, bezbjednosti na internetu, zaštite i medijske pismenosti.

Ključne tačke za razmatranje:

- **Uvod u međusobno povezane koncepte:**
    - Objasnite da računarska bezbjednost, bezbjednost na internetu, zaštita i medijska pismenost nisu izolovani koncepti; često se preklapaju i utiču jedni na druge.
    - Istaknite važnost razumijevanja ovih preklapanja za stvaranje holističkog pristupa digitalnom blagostanju.

Definicije:

- **Računarska bezbjednost:** Zaštita internetski povezanih sistema**,** uključujući hardver, sofver i podatke od računarskih/sajber napada.
- **Bezbjednost na internetu:** Prakse i tehnologije za zaštitu korisnika, posebno djece od opasnosti na internetu, kao što su zlostavljanje na internetu, iskorišćavanje i neprikladan sadržaj.
- **Zaštita**: Mjere za zaštitu pojedinaca, posebno djece i ranjivih odraslih osoba od povrede, zlostavljanja i iskorišćavanja na internetu (*online*) i izvan interneta (*offline*).
- **Medijska pismenost**: Sposobnost pristupa, analize, evaluacije i kreiranja medija u različitim oblicima, uz razumijevanje uloge medija u društvu.

- **Primjeri međusobne povezanosti:**
    - **Pimjer 1: *Fišing* prevare**
        - **Aspekt računarske/sajber sigurnosti:**

Tehničke mjere za otkrivanje i prevenciju fišing pokušaja.

- **Aspekt bezbjednosti na internetu:** Obučiti korisnike da prepoznaju *fišing* e-mailove i da ne klikaju na sumnjive linkove.
- **Aspekt zaštite:** Zaštititi osjetljive informacije od zloupotrebe malicioznih aktera.
- **Aspekt medijske pismenosti:** Razumjeti kako se izvode *fišing* prevare i koji su motivi za to.

- **Primjer 2: Korišćenje društvenih medija**
  - **Aspekt računarske bezbjednosti:** Osigurati da su postavke privatnosti konfigurisane za zaštitu ličnih podataka.
  - **Aspekt bezbjednosti na internetu**: Imati svjest o potencijalnim mogućnostima za sajber zlostavljanje i predatore na internetu**.**
  - **Aspekt zaštite:** Monitoring i usmjeravanje dječjih interakcija na društvenim medijima u cilju njihove bezbjednosti.
  - **Aspekt medijske pismenosti:** Kritička ocjena uočenog sadržaja na društvenim mrežama i razumijevanje njegovog potencijalnog uticaja.

- **Značaj integrisanog pristupa**:
  - Naglasiti da izolovano razmatranje ovih oblasti može dovesti do praznina u zaštiti i obrazovanju.
  - Integrisani pristup osigurava sveobuhvatnu zaštitu i osnažuje korisnike znanjem i vještinama za bezbjedno kretanje u digitalnom svijetu.
- **Praktične implikacije:**
  - **Za edukatore/nastavnike:** Uključite lekcije koje pokrivaju sve ove aspekte kako biste učenicima pružili sveobuhvatno razumijevanje digitalne sigurnosti.
  - **Za roditelje:** Budite informisani i uključeni u dječje aktivnosti na internetu, kombinujući tehničku zaštitu sa otvorenim razgovorima o ponašanju na internetu.
  - **Za kreatore politika:** Izradite politike koje odražavaju međusobnu povezanost ovih oblasti, osiguravajući kohezivne i djelotvorne propise.

Napomene za angažovanje:

- Koristite scenarije iz stvarnog života da biste ilustrovali kako se ovi koncepti ukrštaju u svakodnevnim digitalnim interakcijama.
- Podstaknite učesnike da se angažuju, tako što ćete ih zamoliti da podijele svoja iskustva o bezbjednostii na internetu i izazovima sajber bezbjednosti.
- Dajte praktične savjete i resurse za integraciju ovih aspekata u svakodnevne rutine.

Slajd 24 – Računarske prijetnje školama

Pregled slajda:

- **Sadržaj:** Naglasite da su škole i organizacije koje rade sa djecom glavne mete za sajber-sigurnosne prevare. Navedite relevantne nacionalne podatke o učestalosti povreda podataka.

Ključne tačke za razmatranje:

- **Uvod u prijetnje računarskoj bezbjednosti:** Istaknite sve veći broj napada na sajber sigurnost usmjerenih na škole i organizacije, koje rade s djecom.
- **Povreda podataka u školama:** Navedite da su škole posebno osjetljive na povrede podataka zbog vrijednih ličnih podataka koje posjeduju, kao što su evidencije o učenicima i podaci o osoblju**.**
- **Primjer nacionalnih podataka:**

Zamijenite primjer iz UK relevantnim nacionalnim podacima, koji pokazuju učestalost povreda podataka u školama. [Rezervisano mjesto za nacionalnog konsultanta radi davanja relevantnih informacija].

Primjer: "Nedavni nacionalni podaci ukazuju da se škole značajno više pogođene sajber napadima, u poređenju sa drugim sektorima".

Sve veći broj napada u školama i obrazovnim institucijama:

- Nacionalni podaci iz Crne Gore ukazuju na rastuću prijetnju sajber napada na obrazovne ustanove. Napadi uključuju krađu ličnih podataka učenika, nastavnika i osoblja, kao i prekide u radu sistema upravljanja školama.
- **Primjer:** 2021. godine, Ministarstvo prosvjete, nauke, kulture i sporta prijavilo je incidente u vezi s pokušajima neovlašćenog pristupa bazama podataka učenika u nekoliko osnovnih i srednjih škola. Takođe, određeni softverski alati koji se koriste u školama bili su meta *malvera*, uzrokovanih slabom zaštitom mreža i nedovoljno obučenom IT podrškom.

Povrede ličnih podataka

- Škole su posebno osjetljive zbog arhiviranja podataka kao što su matični brojevi, istorija ocjena, medicinski podaci učenika, pa čak i finansijske informacije. U slučaju sajber napada, ovi podaci mogu postati meta iznude (*ransomware*) ili biti prodati na tamnom *webu.*
- **Podaci iz Crne Gore:** Prema izvještajima nacionalnih tijela, u poslednjih pet godina je registrovano nekoliko pokušaja pristupa elektronskim dnevnicima i sistemima za elektronsku prijavu učenika. Iako većina nije dovela do ozbiljnih povreda podataka, stručnjaci upozoravaju na sve veći rizik jer škole koriste zastarjele sigurnosne sisteme.
- **Razlozi za ciljanje škola:** Diskutujte o tome zašto su škole privlačni ciljevi:
  - Pohranjuju osjetljive lične informacije.
  - Moguće da imaju slabiju zaštitu računarske/sajber bezbjednosti.
  - Ograničeni resursi za strožije mjere računarske bezbjednosti.
- **Efekti povreda sajber bezbjednosti:** Objasnite posljedice neovlašćenog pristupa podacima u školama:
  - Ometanje obrazovnih aktivnosti.
  - Finansijski troškovi dodatne nastave.
  - Gubitak povjerenja roditelja, studenata i osoblja.
  - Mogućnost za krađu identiteta i iskorišćavanje ličnih informacija.
- **Značaj mjera za sajber bezbjednost:**
  - Naglasite potrebu za energičnim praksama računarske bezbjednosti u obrazovnim institucijama.
  - Navedite važnost obučavanja osoblja i učenika u pogledu prepoznavanja i odgovora na sajber prijetnje.

Napomene za učešće:

- Koristite jednostavnu grafiku ili tabelu kako biste ilustrovali porast neovlašćenih pristupa podacima, usmjerenih na škole.
- Podstaknite diskusiju tako što ćete pitati učesnike da li su svjesni bilo kakvih lokalnih incidenata ili mjera koje su škole preduzele za poboljšanje sajber bezbjednosti.

Slajd 25 – Kako se prijetnje manifestuju u školama

- **Uvod:** Ovaj slajd naglašava kako se prijetnje računarske bezbjednosti manifestuju u školama, koristeći podatke iz Ujedinjenog Kraljevstva kao primjer. [Rezervisano mjesto za nacionalnog konsultanta radi davanja relevantnih informacija]. Škole i organizacije koje rade sa djecom sve su sve više na meti sajber prijetnji.
- **Ključne tačke:**
  - ***Fišing napadi***: Značajna većina škola je identifikovala *fišing* napade kao preovlađujuću prijetnju.
  - Nacionalni CERT Crne Gore (CIRT.me) zabilježio je više incidenata pokušaja fišing napada, koji ciljaju obrazovne sisteme, gdje su napadači lažno predstavljali Ministarstvo prosvjete ili školsku administraciju, kako bi dobili pristup osjetljivim podacima.

- **Lažno predstavljanje**: Brojne škole su prijavile incidente u kojima su se sajber kriminalci lažno predstavljali organizacijama, kako bi prevarili pojedince da odaju osjetljive informacije.
- U 2023. godini prijavljeni su incidenti u kojima su sajber kriminalci koristili lažne e-mailove kako bi obmanuli školsko osoblje. Ti napadi uključuju lažno predstavljanje roditelja ili nadležnih institucija kako bi se dobile informacije o učenicima ili finansijama. Takođe, postojao je veći broj lažnih prijava o navodno postavljenim bombama u školama širom Crne Gore.
- **Zlonamjerni softver**: Prijavljeno je prisustvo virusa, špijunskog softvera i drugog zlonamjernog softvera, koji predstavlja rizik za školske podatke i sigurnost mreže.
- Analiza Ministarstva javne uprave pokazala je da je nekoliko osnovnih i srednjih škola imalo problema sa zlonamjernim softverom zbog slabog antivirusnog softvera i neadekvatne obuke školskog IT osoblja.
- U jednoj osnovnoj školi u Podgorici, zlonamjerni softver kompromitovao je bazu podataka učenika i doveo do privremenog prekida u radu elektronskog dnevnika.
- **Neovlašćeni pristup od strane učenika**: Incidenti u kojima su studenti dobili neovlašćeni pristup fajlovima ili mrežama su takođe vrijedni pažnje.
- Zabilježeni su slučajevi u kojima su učenici, koristeći osnovne IT alate, stekli neovlašćeni pristup internim mrežama ili fajlovima škole. Ovi incidenti često nisu bili motivisani zlom namjerom, već radoznalošću, ali ukazuju na slabe tačke u bezbjednosti mreže.
- *Ransomware/hakovanje radi otkupa (ransome, eng.) napadi: Ransomware napadi, gdje se podaci šifriraju (enkriptuju) i drže kao zalog radi otkupa, takođe predstavljaju zabrinutost za obrazovne institucije.*

- **Zaključak:** Ovi primjeri naglašavaju značaj snažnih mjera računarske bezbjednosti u školama i organizacijama koje rade sa djecom. Ove ustanove moraju ostati oprezne i proaktivne u zaštiti od ovih prijetnji, koje se usložnjavaju.

Napomena: Zamijenite podatke iz UK relevantnim nacionalnim podacima, kako bi se bolje prikazale lokalne prijetnje i scenariji.

Iako podaci o napadima specifično usmjerenim na obrazovni sektor u Crnoj Gori nisu široko dokumentovani, Ministarstvo javne uprave i Nacionalni CERT (CIRT.me) upozoravaju na sledeće prijetnje kao relevantne za sve sektore:

Distribuirani napadi uskraćivanja usluge (DDoS):

- Ovi napadi se često koriste za preopterećenje školskih mreža, što može zaustaviti nastavu na daljinu, ometati komunikaciju između nastavnika i učenika i izazvati značajne prekide u radu. Škole sa slabijom infrastrukturom lako postaju meta.

Izloženost podataka zbog lošeg upravljanja IT resursima:

- Loše upravljanje školskim bazama podataka ili nedostatak procedura zaštite može dovesti do nenamjernog izlaganja osjetljivih informacija putem javno dostupnih dokumenata ili neosiguranih servera.

Socijalni inženjering:

- Napadači mogu ciljati osoblje škole, koristeći manipulaciju i prevaru kako bi stekli pristup povjerljivim podacima. Ovo uključuje telefone, e-poštu ili čak lične razgovore.

Napadi preko IoT uređaja (Internet of Things):

- Škole sve više koriste pametne uređaje za sigurnost i učenje (npr. kamere, projektore ili pametne ploče). Ovi uređaji, ako nisu pravilno osigurani, mogu biti zloupotrebljeni za špijunažu ili sabotažu.

Softverske ranjivosti:

- Zastarjeli ili nepodržavani softver u školama može imati sigurnosne propuste koje napadači koriste za kompromitovanje mreža.

Problemi s bezbjednošću u oblaku:

- Upotreba *cloud* servisa za pohranjivanje podataka o učenicima i predavanja nosi rizik od napada na te platforme, ako ne postoji odgovarajuća zaštita.

Slajd 26 – Dezinformacije i netačne informacije

- **Uvod u dezinformacije i netačne informacije:**
  - **Netačne informacije:** Odnose se na lažne ili netačne informacije koje se šire bez zle namjere. To se može dogoditi kroz glasine, nesporazume ili neprovjerene informacije koje se dalje dijele.
  - **Dezinformacije** se namjerno stvaraju i šire sa namjerom radi obmane ili dovođenja u zabludu. To može uključivati izmišljene priče, izmanipulisani sadržaj i koordinisane kampanje radi uticaja na javno mnjenje ili ponašanje.
- **Uticaj na djecu:** Netačne informacije i dezinformacije mogu imati značajan uticaj na decu, utičući na njihovo ponašanje, mentalno zdravlje i percepciju stvarnosti. Djeca su posebno ranjiva zbog njihovog razvijanja vještina kritičkog razmišljanja i veće vjerovatnoće da će povjerovati sadržaju na internetu.
- **Studija slučaja: Izazov plavog kita (2017.):**
  - **Pozadina:** Izazov plavog kita (*The Blue Whale Challenge, eng.)* je bila navodna internetska igra koja je trebala da veličala samoubistvo i uključivala 53 izazova, koja su bila sve ekstremnija i koja su kulminirala samoubistvom učesnika.
  - **Prijavljeni uticaj:** Tvrdilo se da je 150 djece u Ruskoj Federaciji izvršilo samoubistvo kao rezultat učešća u ovom izazovu.
  - **Realnost**: Kasnije je otkriveno da je izazov plavog kita izmišljena priča. Uprkos brojnim upozorenjima i povećanoj svijesti o tome, nije bilo značajnih dokaza koji bi podržali postojanje takvog izazova.
  - **Lekcija:** Ovaj slučaj ilustruje kako dezinformacije mogu stvoriti široko rasprostranjenu paniku i strah, koji pogađaju i djecu i odrasle. Ističe važnost provjere informacija prije njihovog daljeg širenja.
- **Drugi primjeri: Momo Izazov (2019.):**
  - Slično izazovu Plavi kit, Momo izazov (*Momo Challenge*, *eng*.) je uključivao prijave o igri koja je ohrabrivala djecu da izvode opasne zadatke, što je na kraju dovelo do samopovređivanja ili samoubistva.
  - Izazov je govorio o jezivom liku, "Momo", o kojem se naširoko izvještavalo u medijima, stvarajući strah među roditeljima i djecom.
  - Međutim, takođe je razotkriveno da je u pitanju obmana, bez potvrđenih slučajeva sa posljedicom povređavanja djece.

Zaključak:

- Ovi primjeri pokazuju moć i opasnost dezinformacija i netačnih informacija u digitalnom dobu. Od ključne je važnosti edukovati djecu o kritičkom razmišljanju i važnosti provjere informacija iz pouzdanih izvora.
- Kao vaspitači i staratelji, moramo ostati oprezni i proaktivni u borbi protiv širenja lažnih informacija kako bismo zaštitili dobrobit djece.

Slajd 27 – Maltretiranje (zlostavljanje, nasilje) na internetu

- **Uvod u maltretiranje na internetu:**
  - Maltretiranje na internetu, takođe poznato i kao "sajber maltretiranje", uključuje korišćenje digitalnih platformi kao što su društveni mediji, aplikacije za razmjenu poruka i zajednice za igre, u cilju uznemiravanja, prijetnji ili ponižavanja pojedinaca.
  - Za razliku od tradicionalnog maltretiranja, maltretiranje na internetu može se odvijati 24/7 i brzo dostići do šire ciljne grupe, pogoršavajući svoj uticaj na žrtve.
- **Pregled ovog pitanja:**
  - **Rasprostranjenost:** Maltretiranje na internetu je sveprisutan problem koji pogađa djecu i adolescente širom svijeta. Može imati različite oblike, uključujući širenje glasina, dijeljenje privatnih informacija, slanje prijetećih poruka i stvaranje štetnog sadržaja o žrtvi (uključujući sadržaj seksualne prirode).
  - **Uticaj na žrtve:** Psihološki efekti zlostavljanja na mreži mogu biti ozbiljni, što može dovesti do anksioznosti, depresije, niskog nivoa samopoštovanja, pa čak i do suicidalnih misli. Žrtve se često osjećaju nemoćno i izolovano, jer zlostavljanje može biti nemilosrdno i teško ga je izbjeći.

- **Dokazi i statistika:**
  - Prema **Global Kids Online**[2], značajan broj djece doživljava maltretiranje na internetu. U njihovoj studiji je utvrđeno da je:
    - **35%** djece, uzrasta 9-17 godina, prijavilo je maltretiranje na internetu u prošloj godini.
    - **24%** je tvrdilo da su biio često maltretirani.
  - Druga studija "**Cyberbullying Research Center**"[3] navodi da je **37%** učenika doživjelo maltretiranje na internetu tokom svog života, dok je **30%** imalo takvo iskustvo više od jednog put.
  - **UNICEF**[4] takođe naglašava da je veća vjerovatnoća da će djeca koja doživljavaju maltretiranje na internetu izbjegavati školu, ostvariti loš uspjeh u učenju i razviti probleme mentalnog zdravlja (pogledajte kasnije slajd o uticaju SIZDI-ja na žrtve).
- **Studije slučaja i primjeri iz stvarnog života:**
  - **Amanda Todd (2012.):** Amanda Todd, 15-godišnjakinja iz Kanade, podijelila je svoje iskustvo sa maltretiranjem na internetu putem *YouTube* videa. Bila je žrtva sajber maltretiranja i seksualnog iznuđivanja što je dovelo do teške depresije i na kraju njenog samoubistva. Njena priča skrenula je značajnu pažnju na pitanje maltretiranja na internetu i potrebu za preventivnim mjerama.
  - **Megan Meier (2006.)**: Megan Meier, 13-godišnjakinja iz Sjedinjenih Država, uznemiravana je putem lažnog *MySpace* naloga koji je kreirao susjed. Nemilosrdno maltretiranje dovelo je do njenog samoubistva, naglašavajući opasnosti anonimnog uznemiravanja na internetu.

Interaktivnost: Diskusija– da li je neko vidio primjere maltretiranja na internetu/ sajber maltretiranja?

Zaključak:

- Pitanje maltretiranja na internetu naglašava potrebu za sveobuhvatnim obrazovanjem o digitalnoj pismenosti i sistemima podrške žrtvama. Škole, roditelji i kreatori politika moraju zajedno raditi na stvaranju bezbjednog internet okruženja za djecu.
- Podsticanje otvorene komunikacije, podučavanje o empatiji i poštovanju i sprovođenje strogih politika protiv maltretiranja su ključni koraci u borbi protiv zlostavljanja na internetu.

Slajd 28 – Štetan sadržaj na internetu

- **Uvod:**
  - Štetni sadržaj na internetu može značajno uticati na mentalno zdravlje, ponašanje i opštu dobrobit djece.
  - U ovom odjeljku se navode konkretni primjeri radi ilustracije različitih vrsta štetnog sadržaja sa kojim se djeca mogu susresti na mreži.
- **Primjeri štetnog sadržaja na internetu:**
  - **Sadržaj koji sadrži nasilje:**
    - Izloženost video snimcima sa nasiljem, slikama i igrama.
    - Može smanjiti osjetljivost djece na nasilje i dovesti do agresivnog ponašanja.
  - **Seksualni sadržaj:**
    - Pristup pornografiji i eksplicitnom materijalu (većina američkih tinejdžera je izjavila da je vidjela pornografiju sa 13 godina).
    - Može dovesti do iskrivljene percepcije seksa i odnosa, te neprikladnog seksualnog ponašanja, ili čak do trauma (zavisno od prirode ovog sadržaja).
  - **Govor mržnje:**
    - Sadržaj koji promoviše rasizam, ksenofobiju i druge oblike diskriminacije.

2 International day against violence and bullying | Global Kids Online
3 Cyberbullying Data 2019 - Cyberbullying Research Center
4 Cyberbullying: What is it and how to stop it | UNICEF

        - Može usaditi štetne predrasude i podstaknuti isključujuće ponašanje.
    - **Samopovređivanje i samoubistvo:**
        - Web stranice i forumi koji promovišu samopovređivanje, poremećaje u ishrani i samoubistva.
        - Primjeri uključuju izazov Bijelog kita (*Blue Whale Challenge, eng.)* i druge viralne trendove koji veličaju samopovređivanje.
    - **Netačne informacije i dezinformacije**:
        - Lažne informacije o zdravlju, nauci i aktuelnim događajima.
        - Mogu dovesti do opasnih ponašanja i nepovjerenja u vjerodostojne izvore.
- **Tačke za diskusiju:**
    - **Uticaj na djecu:**
        - Psihološke traume, anksioznost, depresija i drugi problemi mentalnog zdravlja.
        - Promjene u ponašanju, uključujući povećanu agresiju ili povlačenje.
    - **Uloga roditelja i edukatora/vaspitača:**
        - Značaj praćenja online aktivnosti i otvorenih razgovora sa djecom (prepoznavanje djece koja su izložena štetnom sadržaju).
        - Podučavanje vještinama kritičkog razmišljanja, kako bi se raspoznale vjerodostojne informacije od štetnog sadržaja.
        - Predlaganje odgovarajućeg odgovora djeci koja su izložena štetnom sadržaju, ili su uključena u takav sadržaj (psihološki, pravni, itd.).

Završne napomene: Sada ćemo istražiti neke studije slučaja kako bismo prikazali probleme i uticaj koji štetni sadržaj ima na djecu.

Slajd 29 – Slučaj Molly Russell

- **Uvod:**
    - Tragičan slučaj koji naglašava uticaj štetnog sadržaja na internetu na omladinu.
    - Fokus je na Molly Russell, 14-godišnjoj djevojčici, koja je sebi oduzela život, 2018. godine.
    - Napomena – ovi primjeri slučajeva su opširno pokriveni u javnim medijima. Budite oprezni sa identitetom djece.
- **Pregled slučaja:**
    - **Detalji o incidentu:**
        - Molly Russell je umrla izvršivši samoubistvo, u novembru 2017. godine.
        - Istraga mrtvozornika 2018. godine otkrila je ključne uvide u faktore koji su doprinijeli njenoj smrti.
    - **Uticaj na sadržaj na internetu:**
        - Otkriveno je da je Molly pogledala preko 2.000 depresivnog sadržaja, samoubilačkog ili sadržaja samopovređivanja na platformama, kao što su *Instagram* i *Pinterest*.
        - Mrtvozornik je zaključio da je ovo izlaganje značajno uticalo na njenu odluku da sebi oduzme život.
- **Ključne tačke:**
    - **Uključene platforme:**
        - *Instagram* i *Pinterest* su naročito pomenuti tokom istrage.
        - Ove platforme imaju algoritme koji mogu nenamjerno promovisati štetan sadržaj, neprestanim sugerisanjem sličnog materijala na osnovu prethodnih interakcija.
    - **Vrste sadržaja:**

        - Depresivne objave, slike samopovređivanja i sadržaji koji pobuđuju suicidne ideje.
        - Sam obim i priroda sadržaja djelovali su kao negativna podrška.
- **Tačke za diskusiju:**
    - **Efekat algoritama:**
        - Kako algoritmi društvenih medija mogu stvoriti štetni eho efekat za ranjive pojedince.
        - Važnost regulisanja i praćenja sadržaja koji ovi algoritmi promovišu.
    - **Uloga kompanija drušvenih medija:**
        - Diskusija o odgovornosti platformi društvenih medija da zaštite svoje korisnike.
        - Radnje koje su ove kompanije preduzele nakon incidenta, kao što je primjena strožijih politika kontrole i upravljanja sadržaja i nuđenje resursa za mentalno zdravlje.
    - **Preventivne mjere:**
        - Značaj roditeljskog nadzora i otvorene komunikacije o aktivnostima na internetu.
        - Škole i zajednice treba da pruže podršku i edukaciju o prepoznavanju i postupanju sa štetnim sadržajem na internetu.

Završne napomene:

- Slučaj Molly Russell predstavlja snažan podsjetnik na stvarne životne posljedice štetnog sadržaja na internetu.
- Naglašava potrebu saradnje između roditelja, edukatora, kompanija društvenih medija i kreatora politika, kako bi djeca i adolescenti bili zaštićeni na internetu.

Slajd 30 – Slučaj Frankie Thomasa

- **Uvod:**
    - Još jedan tragičan primjer koji ilustruje ozbiljne posljedice online aktivnosti bez nadzora i nedostatka odgovarajućih mjera zaštite.
    - Fokus je na Frankie Thomas, 15-godišnjoj djevojčici, sa autizmom, koja je sebi oduzela život 2017. godine.
- **Pregled slučaja:**
    - **Detalji incidenta:**
        - Frankie Thomas je bila učenica u nezavisnoj specijalnoj školi koja je osmišljena da zadovolji njene potrebe zbog njenog autizma.
        - Uprkos tome što je u školi bila cijele sedmice, ona je pohađala samo 1 do 2 predavanja sedmično.
    - **Korišćenje iPad-a:**
        - Škola joj je obezbijedila iPad tokom boravka u njoj.
        - Na ovom uređaju, koji je u vlasništvu i pod upravljanjem škole, Frankie je pristupala raznim vrstama sadržaja, uključujući samoubilački materijal.
- **Ključne tačke:**
    - **Nedostatak kontrola:**
        - Mrtvozornik je otkrio da je škola vjerovala da je korišćenje iPad-a pod roditeljskim nadzorom i filtriranjem sadržaja, ali u stvarnosti nije bilo nikakvog nadzora.
        - Ovo je omogućilo Frankie da slobodno pristupa štetnom sadržaju, što je doprinijelo njenoj odluci da oduzme sebi život kasnije tog dana.
    - **Svijest o ranjivosti:**
        - Škola nije prepoznala da različita djeca imaju različite nivoe ugroženosti na internetu.
        - Ovaj nedostatak razumijevanja i odgovarajuće akcije doprinio je tragičnom ishodu.

- **Teme za diskusiju:**
  - Uloga škola
    - Značaj škola u obezbjeđivanju bezbjednog digitalnog okruženja za sve učenike, posebno one sa posebnim potrebama.
    - Potreba za sveobuhvatnim politikama digitalne bezbjednosti, uključujući djelotvornu upotrebu roditeljskog nadzora i filtriranja sadržaja.
  - **Roditeljska kontrola i filtriranje:**
    - Isticanje kritične uloge roditeljskog nadzora i filtriranja sadržaja na uređajima koje koriste djeca.
    - Potreba za redovnim provjerama i ažuriranjima kako bi se osiguralo da su ove mjere na snazi i učinkovite.
  - **Prilagođene zaštitne mjere:**
    - Potreba za prilagođenim zaštitnim mjerama za zaštitu učenika sa različitim vidovima ranjivosti i potrebama.
    - Osigurati da osoblje i roditelji budu obučeni da prepoznaju i odgovaraju na ove ranjivosti i indikatore viktimizacije, na odgovarajući i blagovremeni način.
- **Preventivne mjere:**
  - **Redovni monitoring:**
    - Naglasiti značaj redovnog praćenja aktivnosti učenika na internetu od strane škola.
    - Implementirati intenzivne obuke o digitalnoj bezbjednosti za školsko osoblje i studente.
  - **Udruženi napori:**
    - Uloga roditelja, vaspitača/nastavnika i kreatora politika u stvaranju sigurnijeg okruženja za decu na internetu.
    - Podsticanje otvorene komunikacije između svih uključenih strana u cilju djelotvornog rješavanja i ublažavanja rizika.

Završne napomene:

- Slučaj Frankie Thomas naglašava hitnu potrebu za rigoroznim mjerama bezbjednosti na internetu u školama.
- Isticanje važnosti razumijevanja i rješavanja jedinstvenih ranjivosti svakog učenika kako bi se spriječile takve tragedije.
- Ovaj slučaj pokazuje da su oni koji su izloženi najvećem riziku na internetu često oni koji suočeni sa najvećim rizikom i van interneta. Sljedeći slajd će pružiti dokaze koji podržavaju ovu tezu.

Slajd 31 – Istraživanje internetskih pitanja: Utočište i rizik

- **Uvod:**
  - Pregled značaja razumijevanja ukrštanja fizičke ranjivosti i rizika na internetu.
  - Uvod u istraživanje organizacije *Internet Matters,* pod nazivom "Utočište i rizik"[5], koje naglašava efekte fizičke ranjivosti na bezbjednost na internetu.
- **Ključni nalazi istraživanja**:
  - **Fizička ranjivost i rizik na internetu:**
    - Djeca koja su ranjiva van interneta (*offline*) zbog fizičkog invaliditeta, problema sa mentalnim zdravljem ili drugih faktora, takođe su izložena većem riziku na internetu (*online*).
    - Ove ranjivosti ih čine podložnijim maltretiranju putem interneta, izloženosti štetnom sadržaju i mamljenju preko interneta.

5 Internet-Matters-Refuge-And-Risk-Report.pdf (internetmatters.org)

- **Statistička evidencija:**
  - Istraživanje pruža podatke koji pokazuju veću učestalost rizika na internetu za fizički ranjivu djecu.
  - Primjeri statistike mogu uključivati veći procenat incidenata maltretiranja na internetu ili izloženosti neprikladnom sadržaju među ovom djecom.

- **Uticaj rizika na internetu na ranjivu djecu:**
  - **Uticaj na mentalno zdravlje:** Izloženost rizicima na internetu može pogoršati postojeće probleme mentalnog zdravlja, prouzrokujući povećanu anksioznost, depresiju i druge psihološke efekte.
  - **Izolacija i isključenost:** Ranjiva djeca se mogu osjećati više izolovano i isključeno, kako na internetu tako i van interneta, zbog svojih iskustava.
- **Studije slučaja i primjeri:**
  - Istaknite specifične slučajeve ili anegdote iz istraživanja koje ilustruju izazove sa kojima se suočavaju fizički ugrožena djeca na internetu.
  - Ovi primjeri pružaju konkretno razumijevanje uticaja rizika na internetu na ovu djecu.
    - 23% [djece sa poremećajima u ishrani] je reklo da je „neko na internetu pokušao da me nagovori na neki oblik seksualne aktivnosti, koji nisam želio". Gotovo trećina je izjavila da je njihovu golišavu sliku podijelio bivši partner u znak osvete nakon raskida.
    - „zbog svog života na internetu (...) 'zaboravim da jedem, pa jedem mnogo i onda se osjećam loše'".
    - (uz napomenu da poremećaji u ishrani mogu biti simptom traume ili post-traumatskog stresnog poremećaja).
- **Preporuke iz istraživanja organizacije *Internet Matters*:**
  - **Unaprijeđene zaštitne mjere:** Srovođenje jačih mjera digitalne zaštite, prilagođenih potrebama fizički ugrožene djece.
  - **Roditeljska i obrazovna podrška:** Obezbjeđivanje resursa i obuke za roditelje i edukatore za bolju podršku i zaštitu ove djece na internetu.
  - **Politika i zagovaranje:** Ohrabrivanje kreatora politika da uzmu u obzir jedinstvene potrebe ugrožene djece u okviru propisa i inicijativa o digitalnoj sigurnosti.
- **Tačke za diskusiju:**
  - Kako škole i roditelji mogu zajedno raditi na ublažavanju ovih rizika?
  - Koji su dodatni resursi i alati dostupni za podršku ugroženoj djeci na internetu?

Završne napomene:

- Naglasiti značaj kontinuiranog istraživanja i proaktivnih mjera za zaštitu fizički ugrožene djece na internetu.
- Naglasiti da rješavanje ovih pitanja zahtijeva zajednički napor roditelja, vaspitača/nastavnika, kreatora politika i tehnološke industrije.

Slajd 32 – Povećana ranjivost u internetskom prostoru

Sadržaj slajda:

- Označite svaku horizontalnu traku, koja predstavlja fizičku ranjivost.
- Objasnite povećanje rizika na internetu za fizički ranjivu djecu.

Klučne tačke za razmatranje:

- **Pregled dijagrama:**
  - Svaka horizontalna traka dijagrama predstavlja određenu fizičku ranjivost.
  - Obojeni blokovi označavaju procenat djece sa tom ranjivošću, koja se suočavaju sa posebnim rizicima na internetu.
- **Primjeri ranjivosti na internetu:**

- **Tamno zelena:** Procenat djece koja se sastaju sa nekom osobom koju su upoznali na internetu.
- **Ljubičasta:** Procenat djece koja koriste pornografiju.

- **Povećanje rizika:**
  - Dijagram ilustruje povećane rizike na internetu kod fizički ranjive djece.
  - Naglasiti kako fizičke ranjivosti mogu dovesti do povećane izloženosti opasnostima na mreži.
- **Opšta ranjivost:**
  - Pojasniti da djeca bez fizičkih nedostataka nisu imuna na rizike na internetu.
  - Istaknuti da se sva djeca mogu suočiti sa prijetnjama na internetu, ali su fizički ranjiva djeca izložena većem riziku.

Tačke za razgovor:

- **Uvod:** Uvedite dijagram, kao dio istraživanja "Internet Matters" o rizicima na internetu sa kojima se suočavaju ranjiva djeca.
- **Objašnjenje dijagrama:**
  - "Svaka od ovih horizontalnih traka predstavlja određenu fizičku ranjivost, kao što su autizam ili poteškoće s mentalnim zdravljem".
  - "Različiti obojeni blokovi unutar svake trake pokazuju procenat djece sa određenim vidom ranjivosti, koja se suočavaju sa specifičnim rizicima na internetu".
- **Primjeri specifičnog vida ranjivosti**: "Na primjer, tamno zeleni blok pokazuje procenat djece koja se sastaju sa nekim koga su upoznali na internetu, dok ljubičasti blok označava one koji koriste pornografiju."
- **Povećanje rizika:** "Ono što ovaj dijagram jasno pokazuje je povećanje rizika na internetu za djecu sa fizičkim ranjivostima. Ova djeca će vjerovatnije doživjeti razne prijetnje na internetu u poređenju sa svojim vršnjacima bez ovih ranjivosti".
- **Univerzalni rizik:** "Važno je napomenuti da dok se fizički ranjiva djeca suočavaju sa većim rizicima, nijedno dijete nije potpuno bezbjedno od opasnosti na internetu. To naglašava potrebu za sveobuhvatnim mjerama bezbjednosti na internetu za svu djecu".

Završne napomene: "Ovaj vizuelni prikaz naglašava kritičnu vezu između fizičkih ranjivosti i povećanih rizika na mreži. Služi kao snažan podsjetnik na potrebu ciljanih intervencija za zaštitu najugroženije djece u našem društvu".

Prateći ove napomene, možete učinkovito prenijeti značajno povećanje *online* rizika za fizički ranjivu djecu, istovremeno naglašavajući univerzalnu prirodu internet prijetnji.

Slajd 33 – Procenat djece izložene različitim rizicima na internetu

Pregled: Ovaj slajd predstavlja podatke iz *Global Kids Online*[6], koji pokazuju procenat djece u različitim zemljama, koja su bila izložena raznim rizicima na internetu. Podaci ističu globalnu prirodu ovih pitanja i naglašavaju značaj rješavanja bezbjednosti djece na internetu, u različitim regijama.

Ključne tačke:

- **Sadržaj samopovređivanja:**
  - Albanija: 18%
  - Bugarska: 18%
  - Čile: 15%
  - Gana: 15%
  - Italija: 22%
  - Filipini: 14%

6 Done right, internet use can increase learning and skills | Global Kids Online[Ukoliko se pravilno koristi, internet može unaprijediti učenje i sticanje vještina-Global Kids Online]

- Južna Afrika: 18%
- Urugvaj: 22%

- **Suicidni sadržaj:**
  - Albanija: 12%
  - Bugarska: 12%
  - Čile: 12%
  - Gana: 16%
  - Italija: 13%
  - Filipini: 20%
  - Južna Afrika: 18%
  - Urugvaj: 16%
- **Govor mržnje:**
  - Albanija: 10%
  - Bugarska: 28%
  - Čile: 21%
  - Gana: 12%
  - Italija: 35%
  - Filipini: 12%
  - Južna Afrika: 34%
  - Urugvaj: 35%
- **Sadržaj sa nasiljem:**
  - Albanija: 35%
  - Bugarska: 26%
  - Čile: 30%
  - Gana: 18%
  - Italija: 33%
  - Filipini: 30%
  - Južna Afrika: 33%
  - Urugvaj: 40%
- **Seksualni sadržaj:**
  - Albanija: 16%
  - Bugarska: 37%
  - Čile: 24%
  - Gana: 39%
  - Italija: 27%
  - Filipini: 22%
  - Južna Afrika: 51%
  - Urugvaj: 36%

Tačke za diskusiju:

- **Globalna perspektiva:**

- Podaci pokazuju da su djeca širom svijeta izložena brojnim rizicima na internetu, bez obzira na njihovu geografsku lokaciju.
- Različiti regioni pokazuju različite nivoe izloženosti određenim vrstama štetnog sadržaja.

- **Implikacije za bezbjednost na internetu:**
  - Razumijevanje ove statistike je ključno za razvoj ciljanih intervencija i obrazovnih programa za zaštitu djece na internetu.
  - Istaknuti potrebu za međunarodnom saradnjom u rješavanju ovih pitanja i razmjeni najboljih praksi.
- **Uključivanje učesnika:**
  - Podstaknite razmišljanja o razlikama između zemalja i razgovarajte o potencijalnim kulturnim, ekonomskim ili regulatornim faktorima koji bi mogli uticati na ove varijacije.
  - Pokrenite pitanja i diskusije o tome kako ovi podaci mogu poslužiti lokalnim i globalnim strategijama za poboljšanje sigurnosti djece na internetu.

Zaključak: Podaci iz *Global Kids Online* naglašavaju univerzalnu prirodu rizika na internetu sa kojima se djeca suočavaju i hitnu potrebu za sveobuhvatnim mjerama za zaštitu njihovog iskustva na internetu.

Slajd 34 – Nacionalni aspekti

- Podaci o bezbjednosti djece na internetu u Crnoj Gori, prema istraživanju Global Kids Online sprovedenom 2016. godine, pokazuju da se 45% djece u Crnoj Gori ne osjeća bezbjedno na internetu.
- 38% njih je doživjelo bar jedno neprijatno iskustvo online u prethodnoj godini.
- Uznemirujući sadržaj i sajber maltretiranje.
- Češće su prijave podnosili dječaci i tinejdžeri nego djevojčice.
- Većina ne zna kako da reaguje u tim situacijama.

5.1 SEKSUALNO ISKORIŠĆAVANJE I ZLOSTAVLJANJE DJECE NA INTERNETU

Slajd 35 – Seksualno iskorišćavanje i zlostavljanje djece na internetu

Opšti uvod

S obzirom na to da je glavni fokus našeg projekta na seksualnom iskorišćavanju i zlostavljanju djece na internetu (SIZDI), ovaj odjeljak ima za cilj pružiti sveobuhvatno razumijevanje različitih aspekata SIZDI-ja.

Razmatraćemo sljedeće oblasti:

- **Seksualno zlostavljanje djeteta:**
  - Ispitati rasprostranjenost i uticaj seksualnog zlostavljanja djece preko internet platformi.
  - Istaknuti ulogu digitalnih tehnologija u iskorišćavanju i zlostavljanju djece.
- **Štetno seksualno ponašanje:**
  - Razumijevanje različitih vrsta neprikladnog i štetnog seksualnog ponašanja koje djeca mogu pokazati ili doživjeti na internetu.
  - Raspravljati o implikacijama takvog ponašanja na mentalno i fizičko blagostanje djece.
- **Procjena prijetnje:**
  - Procjena različitih prijetnji povezanih sa SIZDI-jem.
  - Razumijevanje načina na koji se ove prijetnje procjenjuju i koje mjere su preduzete za njihovo ublažavanje.
- **Iznuda (novčana):**
  - Istražiti kako djeca postaju ciljana grupa za finansijsku iznudu putem internet interakcija.
  - Rasprava o metodama koje počinioci koriste za iznuđivanje novca i osjetljivih informacija od djece.

Ključne tačke za raspravu:

- **Uvod u SIZDI:**
  - Definicija i obim seksualnog iskorišćavanja i zlostavljanja djece na mreži (SIZDI)

    Seksualno iskorišćavanje i zlostavljanje djece na mreži (SIZDI) odnosi se na niz iskorišćavajućih i nasilnih aktivnosti, koje se vrše nad djecom i koje su olakšane putem digitalnih platformih. Ovaj pojam obuhvata različite oblike seksualnog iskorišćavanja, uključujući, ali ne i ograničavajući se na proizvodnju, distribuciju i potrošnju materijala o seksualnom zlostavljanju djece (SIZDM), mamljenje putem interneta u seksualne svrhe, uživo prenošeno seksualno zlostavljanje i iznuđivanje seksualnih radnji ili slika, pod prijetnjom. Zlostavljanje na internetu i van interneta često se isprepliću: ranjiva djeca su u većoj opasnosti od SIZDI-ja, od žrtava se traži da izvrše seksualni čin u stvarnom životu sa ciljem korišćenja digitalnog snimanja istog *online*, (teške) *offline* posljedice se uočavaju na žrtvama, itd.
  - Obim:

- Globalni domet: SIZDI ima prekogranični karakter, što ga čini globalnim pitanjem koje zahtijeva koordinisane međunarodne napore. Počinioci mogu djelovati anonimno sa bilo kojeg mjesta u svijetu, često iskorišćavajući praznine u zakonima o nadležnosti.
- Anonimnost i dostupnost: Internet nudi počiniocima određeni stepen anonimnosti, što u sticaju sa široko rasprostranjenom dostupnošću digitalnih uređaja, olakšava prenos uživo SIZDI-a, kao i brzu proizvodnju, širenje i potrošnju SIZDIM-a. Dostupnost djece na internetu – putem društvenih medija, platformi za igre i komunikacijskih aplikacija – stvara višestruke mogućnosti za počinioce da pristupe žrtvama i da ih namamljuju.
- Složenost identifikacije i krivičnog gonjenja: Digitalna priroda SIZDI-a čini otkrivanje i krivično gonjenje posebno zahtjevnim. Neki počinioci koriste tehnike i tehnologije kako bi izbjegli sprovođenje zakona, uključujući šifriranje (enkripciju), *dark we*b (tamni web) i kriptovalute, što otežava napore da se uđe u trag i obavi identifikacija.

  Djeca sebe često ne vide kao žrtve, plaše se ili se stide istupiti, što otežava njihovu identifikaciju.
- Psihološki i društveni uticaj: SIZDI ima duboke i dugotrajne efekte na žrtve, uključujući psihološku traumu, društvenu stigmatizaciju i poremećaje u normalnom razvoju djetinjstva. Uticaj se proteže izvan pojedinačnih žrtava, pogađajući porodice, zajednice i šire društvo.

- Ovaj uvod ne samo da pruža jasnu definiciju SIZDI-a, već i ističe opsežan i višestruki raspon problema, postavljajući osnovu za dublje istraživanje njegovih različitih dimenzija na sljedećim slajdovima.
- Značaj razmatranja SIZDI-a u kontekstu sve veće upotrebe interneta među djecom.

- **Seksualno zlostavljanje djece:**
  - Oblici seksualnog zlostavljanja djece na internetu (npr. mamljenje, prenos zlostavljanja uživo).
  - Uticaj na žrtve i njihove porodice.
  - Pravna i etička razmatranja.
- **Štetno seksualno ponašanje:**
  - Definicija i primjeri štetnog seksualnog ponašanja na internetu.
  - Psihološki i društveni faktori koji doprinose takvom ponašanju.
- **Procjena prijetnje:**
  - Okviri i metodologije za procjenu prijetnji u vezi sa SIZDI.
  - Uloga organa za sprovođenje zakona i agencija za zaštitu djece u procjeni opasnosti.
- **Iznuda (novčana):**
  - Mehanizmi iznude koji uključuju djecu.
  - Studije slučaja i primjeri iz stvarnog života.
  - Preventivne mjere i roditeljski nadzor.

Zaključak: Ovaj odjeljak pruža osnovno znanje o različitim dimenzijama seksualnog iskorišćavanja i zlostavljanja djece na internetu. Svaka oblast će biti detaljno istražena, naglašavajući izazove, implikacije i zaštitne mjere povezane sa SIZDI. Naredni slajdovi će dublje analizirati svaku od ovih kritičnih oblasti i navesti uvide i strategije za borbu protiv ovih gorućih problema.

Slide 36 - Lanzarot konvencija: Sveobuhvatan okvir za borbu protiv seksualnog nasilja nad djecom

Ključne tačke:

- **Svrha:** Lanzarote konvencija je najobuhvatniji ugovor koji, je posebno usmjeren na zaštitu djece od seksualnog iskorišćavanja i zlostavljanja. Utvrđuje različite oblike seksualnog zlostavljanja djece kao krivična djela, uključujući i ona koja su izvršena u porodici ili primjenom prinude.
- **Implementacija i monitoring:** Konvencija obavezuje Države članice da usvoji posebno zakonodavstvo za sprječavanje, zaštitu i krivično gonjenje slučajeva seksualnog zlostavljanja djece. Poseban komitet, Lanzarot

komitet, ima zadatak da nadgleda efektivnu implementaciju Konvencije i identifikuje najbolje prakse među Državama članicama.

- **Globalni domet:** Lanzarote Konvencija proširuje mogućnost pristupanja na bilo koju zemlju širom svijeta, naglašavajući svoj globalni pristup zaštiti djece od seksualnog nasilja.
- **Pravne i praktične mjere:** Konvencija naglašava stvaranje sigurnog okruženja za djecu, kako u fizičkoj, tako i u digitalnoj sferi, uključivanjem mjera protiv mamljenja i drugih rizika na internetu.

Ova Konvencija odražava čvrstu posvećenost Savjeta Evrope zaštiti prava djece i osiguravanju holističkog pravnog i društvenog pristupa borbi protiv seksualnog zlostavljanja u fizičkom i digitalnom okruženju.

Slajd 37 – Lanzarote Konvencija

Napomene izlagača:

Lanzarot konvencija je najobuhvatniji međunarodni instrument koji se bavi seksualnom eksploatacijom i zlostavljanjem djece. Konvencija navodi ključna krivična djela i propisuje preventivne mjere, mehanizme zaštite i strategije krivičnog gonjenja. Ovo su osnovna krivična djela obuhvaćena Konvencijom:

- **Seksualno zlostavljanje (član 18):** Uključivanje u seksualne aktivnosti sa djetetom starosti ispod zakonske dobi za seksualne aktivnosti, uključujući putem prnude, sile ili prijetnje; zloupotrebom položaja povjerenja ili zloupotrebom osjetljive situacije djeteta zbog ranjivog položaja.
- **Eksploatacija djece putem prostitucije (član 19):** Vrbovanje, navođenje, primoravanje ili iskorišćavanje djeteta da učestvuje u seksualnim aktivnostima radi ostvarivanja naknade.
- **Dječija pornografija / materijal pornografske sadržine (član 20):** Uključuje proizvodnju, nuđenje ili činjenje dostupnim, distribuciju, dijeljenje, uvoz, izvoz, posjedovanje, ili svjesno pristupanje pornografskom materijalu.
- **Učešće djece u pornografskim predstavama (član 21):** Vrbovanje, navođenje, primoravanje djeteta, ili ostvarivanje zarade ili neki drugi vid iskorišćavanja djece za pornografske predstave seksualne prirode, ili svjesno prisustvovanje takvim predstavama.
- **Korumpiranje djece (član 22):** Izlaganje djece ispod zakonske dobi da svjedoče seksualnim aktivnostima, ili seksualnom zlostavljanju.
- **Mamljenje djece u seksualne svrhe (*Grooming, eng.*) (Član 23)**: Sa namjerom pokretanje komunikacije, putem informaciono-komunikacionih tehnologija (IKT), sa djetetom radi seksualnog zlostavljanja, bilo na internetu ili izvan interneta.

Konvencija naglašava potrebu za sveobuhvatnim pravnim i mjerama politike za zaštitu djece od seksualnog iskorišćavanja i zlostavljanja, kako izvan internet,a tako i na internetu.

Nacionalni status Konvencije o pravima djeteta - Convention on the Rights of the Child | OHCHR: Crna Gora je ratifikovala Konvenciju o pravima djeteta i preduzima korake za rješavanje problema koji uključuju sajber 2 i druge oblike nasilja nad djecom u digitalnom prostoru. Sajber nasilje spada pod šire oblike nasilja koje se definišu i tretiraju kroz nacionalne i međunarodne zakone i strategije. Komitet za prava djeteta naglašava da sajber nasilje zahtijeva posebnu pažnju, posebno zbog sve veće digitalizacije društva.

- Zaštita privatnosti (Član 16) - Dijete ima pravo na privatnost. Zabranjeno je miješanje u privatni i porodični život, ličnu prepisku, kao i povrede časti i ugleda djeteta.
- Pristup prikladnim informacijama (Član 17) - Dijete ima pravo da dobije pouzdane informacije iz sredstava javnog informisanja. Televizija, radio i novine treba da pružaju informacije koje su djetetu razumljive i ne smiju promovisati sadržaje koji su štetni za dijete.
- Zaštita od zlostavljanja i zanemarivanja (Član 19) - Vlade moraju osigurati pravilnu njegu djece i zaštititi ih od nasilja, zlostavljanja ili zanemarivanja od strane njihovih roditelja ili nekog drugog ko se o njima stara.
- Seksualno iskorištavanje (Član 34) - Država mora zaštititi djecu od seksualnog iskorišćavanja i zlostavljanja, uključujući prostituciju i angažovanje u pornografiji.
- Prodaja, trgovina i otmica (Član 35) - Država mora učiniti svaki mogući napor da spriječi prodaju, trgovinu i otmicu djece.
- Drugi oblici iskorištavanja (Član 36) - Djeca moraju biti zaštićena od svih aktivnosti koje bi mogle ugroziti njihov razvoj.

Slajd 38 – Ko su žrtve

Uvod:

Napomene izlagača:

- Prema međunarodnim standardima, djeca su lica mlađa od 18 godina. SIZDI se stoga odnosi na zlostavljanje koje je izvršeno nad licima mlađim od 18 godina[7].
- Žrtve mogu biti dječaci ili djevojčice.
- Mogu se identifikovati žrtve svih uzrasta: neke studije pokazuju da tinejdžeri mogu biti više pogođeni[8], dok drugi smatraju da su djeca pred-pubertetskog uzrasta previse zastupljena u SIZDIM-u.[9]

Ključne tačke:[10]

- Kao što je objašnjeno, djeca koja su ranjiva u stvarnom životu često su ranjiva i na internetu. Na primjer: izvještaj *WeProtect*-a iz 2023. godine, otkriva da su "djeca iz manjinskih ili marginalinalizovanih grupa na osnovu njihove seksualne orijentacije, rase, etničke pripadnosti ili invaliditeta, više izložena seksualnim povredama na internetu". Osim toga, žrtve koje su doživjele seksualno zlostavljanje ili druge traume u prošlosti su izložene višem riziku da budu re-viktimizirane, uključujući i internetsko okruženje.
- Žrtve se često biraju iz bliskog okruženja nasilnika (krug povjerenja).
- Manje je vjerovatno da će tinejdžeri prijaviti zlostavljanje odraslim osobama, nego djeca mlađe dobi.

Zaključak:

- Važno je ne razdvajati zlostavljanje na internetu i izvan interneta.
- Stručnjaci bi trebalo da redovno procjenjuju ranjivost djece, kako bi uspješnije otkrivali one koji su pod rizicima, kao i žrtve.
- Obrazovni napori treba da budu usmjereni na svu djecu sa porukama prikladnim uzrastu, kao i da šire - na njihove roditelje.

Slide 39 – Mamljenje djeteta (nagovaranje) (Grooming, eng.)

Uvod:

- Ovaj slajd se fokusira na mamljenje: kako ljudi mogu mamiti djecu na raznim platformama na internetu, sa ciljem da ih uključe u seksualnu aktivnost.
- Mamljenje preko interneta se dešava kada lice ostvaruje komunikaciju sa djetetom na internetu kako bi izgradila povjerenje i izmanipulisala dijete da učestvuje u seksualnim aktivnostima.

Ključne tačke:[11]

- Djeca se mogu mamiti preko interneta, izvan interneta, ili na oba načina.
- Mamljenje na internetu ima za cilj da seksualna ponašanja predstavi normalnim i da uključi dijete u seksualne aktivnosti na internetu (sa kamerom) ili izvan interneta (sastanak u stvarnom životu), ili dijeljenje seksualnog sadržaja koji je sam/a napravio/la.
- Da bi ostvarili taj cilj, lica koja vrše mamljenje (*groomers*, eng.), mogu ćaskati (*chat*) sa djetetom, pokazati svoj pornografski ili seksualni sadržaj, uplašiti dijete itd.

7 https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child
8 Disrupting Harm – ECPAT, INTERPOL
9 https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf
10 https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf; https://www.weprotect.org/economist-impact-parents-survey/
11 Vidjeti takođe: https://inhope.org/EN/articles/the-stages-of-grooming

- Na internetu, djeca se često namaljuju aplikacijama za razmjenu poruka, društvenim medijima, aplikacijama za upoznavanje ili platformama za igre (npr. *Instagram, Facebook, Discord, Whatsapp, Telegram, Grindr, Fortnite, Minecraft, Roblox, VRChat*, itd.)[12].
- Lica koja se bave mamljenjem su češće punoljetne osobe, ali mogu biti i djeca. Mogu biti stranci, pretvarati se da su neko drugi (uključujući i dijete) ili biti poznati djetetu.

Tačke za diskusiju:

- Ohrabrite učesnike da razgovaraju sa djecom o ključnim granicama koje treba da uspostave: da nikada ne pristaju na lične sastanke bez konsultacije sa odraslom osobom i da nikada ne dijele intimne sadržaje na mreži.
- Razgovarajte o značaju svijesti o rizičnim aplikacijama i web stranicama, kao i o razumijevanju ponašanja djece na internetu.

Zaključak:

- Zaključite naglašavanjem značaja održavanja kontinuiranog dijaloga sa djecom i razumijevanja indikatora seksualnog iskorišćavanja i zlostavljanja djece na internetu (SIZDI) u cilju olakšanja rane identifikacije žrtava.

Slajd 40 – Materijal o seksualnom zlostavljanju djece (SIZDM)

Napomene izlagača:

Uvod:

- Materijal o seksualnom zlostavljanju djece (SIZDM) predstavlja ozbiljno kršenje prava djece i značajno je globalno pitanje – često se pogrešno naziva dječjom pornografijom.
- Termin "Materijal seksualnog zlostavljanja djece (SIZDM)" se namjerno koristi umjesto "dječje pornografije" kako bi se preciznije i suptilnije opisala priroda krivičnog djela i njegov uticaj na žrtve. Odabir termina SIZDM se zasniva na nekoliko glavnih razloga:
    1. Prepoznavanje težine krivičnog djela: Termin "Dječja pornografija" je zavaravajući, jer može implicirati sporazumni ili legalni oblik pornografije, umanjujući ozbiljnost krivičnog djela. Nasuprot tome, "Materijal o seksualnom zlostavljanju djece" eksplicitno identifikuje materijal kao dokaz kriminalne aktivnosti i zlostavljanja, naglašavajući težinu ovog krivičnog djela.
    2. Priznanje patnji žrtve: Pozivanje na takav sadržaj kao "pornografiju" može zamagliti činjenicu da postoji stvarno dijete koje je zlostavljano i iskorišćavano. Izraz "SIZDM" usredsređuje se na dijete kao žrtvu zlostavljanja, a ne kao učesnika u pornografiji, ističući prisilnu i zlostavljačku prirodu djela.
    3. Akcenat je na zlostavljanju, a ne na sadržaju: "Dječja pornografija" sugeriše fokus na sam sadržaj, dok "SIZDM" naglašava zlostavljačke i nezakonite radnje koje proizvode takav materijal. Izraz "SIZDM" jasno daje do znanja da se radi o zlostavljanju djece, a ne o proizvodnji bilo kojeg oblika "zabave".
    4. Pravne i društvene implikacije: Upotreba termina "Dječja pornografija" može produžiti štetne zablude, potencijalno dovesti do manje osude javnosti i blaže zakonske kazne. Koristeći "SIZDM", terminologija je usklađena sa pravnim okvirima i međunarodnim standardima koji priznaju pun obim krivičnog djela, osiguravajući da se sa njim postupa sa ozbiljnošću kakvu i zaslužuje.
    5. Globalni konsenzus i najbolje prakse: Međunarodne organizacije, uključujući Ujedinjene nacije, Interpol i Savjet Evrope, zalažu se za korišćenje „Materijala o seksualnom zlostavljanju djece" kako bi se osigurao dosljedan pristup rješavanju ovog zločina, usmjerenog na žrtve. Ova terminologija je dio širih napora da se standardizuju odgovori na seksualno iskorišćavanje djece na internetu i da se prioritizuju zaštita i dostojanstvo žrtava. Relevantne termine koji se koriste kada se govori o SIZD i odgovarajuće definicije, ove organizacije su objedinile u "Luksemburške smjernice" .
- Ukratko, termin "Materijal o seksualnom zlostavljanju djece (SIZDM)" nije samo precizniji opis, već i ključno sredstvo u preobličavanju razgovora o ovim krivičnim djelima. Osigurava da jezik koji koristimo odražava pravu prirodu krivičnog djela, štetu za žrtve i hitnu potrebu za snažnim pravnim i društvenim odgovorima.

12 https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf
https://unicri.it/sites/default/files/2022-11/Gaming%20and%20the%20Metaverse.pdf
https://safeonline.global/disrupting-harm/

- Ovaj slajd naglašava obim i uticaj SIZDM, naglašavajući potrebu za povećanom sviješću i preventivnim mjerama.

Ključne tačke:

- **Definicija i obim:**
  - SIZDM se odnosi na bilo koji materijal seksualne prirode ili je korišćen u seksualne svrhe koji prikazuje dijete[13].
  - Uključuje slike, video zapise i druge digitalne zapise proizvedene, podijeljene i ili distribuirane na internetu.
- **Rasprostranjenost**:
  - Problem SIZDM je sveprisutan, sa milionima izvještaja u godini.
  - 2022. godine, Nacionalni centar za nestalu i iskorišćavanu djecu analizirao je 32 miliona izvještaja o SIZDM-u, naglašavajući opsežnu prirodu ovog pitanja.
  - SIZDM se može naći u značajnom obimu na otvorenom internetu, što ga čini dostupnim svima.
- **Izvještavanje i otkrivanje:**
  - Organizacije kao INHOPE Hotlines[14], Internet Watch Foundation (IWF), INTERPOL, EUROPOL, imaju ključnu ulogu u otkrivanju i uklanjanju SIZDM-a.
  - Grafikon na slajdu prikazuje trendove u izvještajima o dječjim slikama u posljednjih nekoliko godina, što odražava alarmantno povećanje.
  - Važno je napomenuti da SIZDM često prikazuje seksualno zlostavljanje djece iz stvarnog života i da nije samo pitanje interneta. To ukazuje da je dijete u opasnosti. Stoga, poduzimanje radnji nakon otkrivanja SIZDM-a podrazumijeva više od samog uklanjanja materijala ili blokiranja njegovog kruženja; to takođe zahtijeva rješavanje osnovnog zlostavljanja i zaštitu djeteta, ukoliko je to je moguće.
  - Kako prepoznati da li je SIZDM nezakonit (za potrebe izvještavanja): može biti izazovno utvrditi jesu li fotografija ili video nezakoniti, pogotovo zato što SIZDM ima prekogranični karakter, a zakoni se razlikuju od zemlje do zemlje. Međunarodni standardi koje je razvio INTERPOL i koje koriste profesionalci širom svijeta mogu pomoći u ovom procesu. Shodno ovim standardima, fotografija ili video se svuda smatra nezakonitim ako:
    - Prikazuje stvarno djete pred-pubertetskog uzrasta.
    - I prikazuje genitalna ili analna područja, ILI seksualne aktivnosti.

    To ne znači da je proizvodnja, posjedovanje ili dijeljenje takvog materijala prihvatljivo kada je prikazano dijete tinejdžer, ali bi ipak moglo pomoći kod odlučivanja koju radnju preduzeti.
- **Tehnološki izazovi:**
  - Napredak u tehnologiji, uključujući tamne mreže (*dark web)* i enkripciju, te korišćenje P2P-a, olakšali su izvršiocima da dijele SIZDM dok izbjegavaju sprovođenje zakona.
  - Razvijaju se alati vještačke inteligencije i uređaja, kako bi se djelotvornije spriječila distribucija SIZDM-a.
- **Uticaj na žrtve:**
  - Žrtve SIZDM-a trpe dugoročne psihološke, emocionalne i socijalne posljedice.
  - Zlostavljanje često traje, jer se fotografije u iznova dijele i gledaju, uzrokujući ponovljene i beskrajne traume.

---

13 Direktiva EU 2011/93 upućuje, u svojoj Preambuli, na činjenicu da „dječja pornografija često uključuje fotografije koje snimaju seksualno zlostavljanje djece od strane odraslih", ali tvrdi da dječja pornografija može biti i nešto šire, dodajući „[i] može takođe uključivati i fotografije djece uključene u seksualno eksplicitno ponašanje, ili njihovih polnih organa, kada se takve slike proizvode ili koriste u prvenstveno seksualne svrhe i iskorišćavaju se sa znanjem ili bez znanja djeteta. Nadalje, u koncept dječje pornografije takođe spadaju realistične slike djeteta, gdje je dijete angažovano ili prikazano kao uključeno u seksualno eksplicitno ponašanje, prvenstveno u seksualne svrhe" (Uvod paragraf 8)": Luksemburške smjernice, str. 39: https://ecpat.org/terminology/

14 inhopenetwork_hotlinedirectory.pdf

- **Pravne i zaštitne mjere:**
  - Globalna saradnja i strogi zakoni su ključni u borbi protiv SIZDM-a, kao i napori privatnog sektora da na odgovarajući način reguliše korišćenje svojih usluga.
  - Napori takođe uključuju oštrije kazne za izvršioce krivičnih djela i sisteme podrške žrtvama.
  - Radna mjesta takođe mogu igrati značajnu ulogu u otkrivanju SIZDM-a na radnim uređajima.

Zaključak:

- SIZDM je kritično pitanje, koje zahtijeva višestrani pristup, koji uključuje sprovođenje zakona, tehnologiju i svijest javnosti.
- Naglasiti potrebu za kontinuiranom budnošću i djelovanjem u cilju zaštite od takvog gnusnog iskorišćavanja.

Slajd 41 – Materijal o seksualnom zlostavljanje djece

Ključne tačke:

- Rasprostranjenost materijala o seksualnom zlostavljanju djece (SIZDM) je značajan problem na globalnom nivou.
- Brojni akteri su ključni u borbi protiv SIZDM-a, npr. Internet Watch Foundation (IWF), INHOPE, NCMEC, Thorn, INTERPOL, EUROPOL, nacionalne telefonske linije i nacionalna policija.
- Najnoviji podaci pokazuju drastičan porast broja prijava i potvrđenih slučajeva SIZDM-a.
- 2023 CyberTipline Reports by Country (missingkids.org) - lokacija SIZDM sadržaja prijavljenog NCMEC-u.
  - Gruzija 15.055
  - Moldavija 30.972
  - Crna Gora 8.490

Detaljne tačke za razmatranje:

- **Problem i rasprostranjenost SIZDM-a:**
  - Porast dostupnosti i distribucije SIZDM-a je alarmantan, što ukazuje na rastuću prijetnju sigurnosti djece na internetu.
- **IWF podaci i analiza**:
  - Internet Watch Foundation (IWF) i WeProtect izvijestili su o značajnom povećanju broja primljenih izvještaja i potvrđenih slučajeva SIZDM-a od 2019. do 2023. godine.
  - U 2023. godini, IWF je primio 392.660 prijava, od kojih je značajan dio potvrđen da sadrži nezakoniti sadržaj.
  - Primjetan je porast samogenerisanog sadržaja, posebno među djecom mlađeg uzrasta. Podaci pokazuju povećanje od 1000% u slikama koje uključuju djecu starosti od 7 do 10 godina.
- **Samogenerišući sadržaj:**
  - Značajan dio potvrđenog SIZDM-a je samogenerisan, često uključuje djecu koja su prisiljena ili namamljena da stvaraju eksplicitni materijal.
  - Povećanje samogenerisanog sadržaja postavlja nove izazove za prevenciju i intervenciju.

Vizuelni podaci:

- **Trakasti grafikon:**
  - Trakasti grafikon na lijevoj strani ilustruje broj prijava podnijetih IWF-u, po godinama (2019-2023).
  - Srednji grafikon prikazuje potvrđene prijave, koje sadrže nezakonit sadržaj.
  - Desni grafikon naglašava porast samogenerisnog sadržaja, pri čemu značajan broj uključuje vrlo malu djecu.

Ključne statistike:

- **Primljene prijave:**
  - 2019: 260,400
  - 2020: 299,600
  - 2021: 361,000
  - 2022: 375,230
  - 2023: 392,660
- **Potvrđene prijave:**
  - 2019: 132,700
  - 2020: 153,350
  - 2021: 252,000
  - 2022: 255,570
  - 2023: 275,655
- **Označeno kao samogenerisano:**
  - 2019: 38,400
  - 2020: 68,000
  - 2021: 182,000
  - 2022: 199,360
  - 2023: 254,070

Važna napomena: Podaci naglašavaju rastući problem, jer su djeca mlađeg uzrasta, od 7-10 godina, sve više zastupljena u samogenerisanom SIZDM-u, naglašavajući hitnu potrebu za snažnim zaštitnim mjerama.

Zaključak: Ovaj odjeljak naglašava ozbiljno i eskalirajuće pitanje materijala o seksualnom zlostavljanju djece (SIZDM), naglašavajući ključnu ulogu praćenja, prijavljivanja i preventivnih mjera u zaštiti djece od iskorišćavanja na internetu.

Tokom obavljanja svojih profesionalnih dužnosti, možete naići na cirkulaciju SIZDM-a u koji su uključena djeca pod vašim nadzorom, ili kolega. Ključno je preduzeti mjere uz očuvanje digitalnih dokaza, kako biste izbjegli kompromitaciju bilo koje moguće istrage (ovo će biti detaljno opisano drugog dana obuke).

Slajd 42 – Vještačka inteligencija i materijal o seksualnom zlostavljanju djece (SIZDM)

Uvod:

- U oktobru 2023. godine, *I*nternet Watch Foundation (IWF) je objavila izvještaj koji naglašava alarmantnu upotrebu AI (eng. skraćenica - *artificial intelligence* - vještačka inteligencija) za kreiranje materijala o seksualnom zlostavljanju djece (SIZDM).[15]
- Ova studija manjeg obima fokusirala se na jedan dark web forum, otkrivajući 10.500 sintetičkih SIZDM slika, od kojih je 2.500 zadovoljilo zakonski prag u Velikoj Britaniji za SIZDM.

Ključni nalazi:

- **Razmjere problema:** Izvještaj je pokazao značajan obim sintetičkog SIZDM-a, koji se generiše i dijeli na mračnim web platformama.
- **Pravne implikacije**: značajan broj ovih fotografija se kvalifikuje kao nezakonit po zakonodavstvu Ujedinjenog Kraljevstva, naglašavajući ozbiljnost prijetnje koju predstavlja sadržaj generisan vještačkom inteligencijom.

15 How AI is being abused to create child sexual abuse material (CSAM) online (iwf.org.uk)

- **Trendovi u nastajanju**: Centar za sigurniji internet u Ujedinjenom Kraljevstvu izvijestio je u novembru 2023. godine da djeca sve više koriste AI i aplikacije/usluge "nudifikacije" za kreiranje SIZDM-a svojih vršnjaka. Ovi alati digitalno uklanjaju odjeću sa slika, stvarajući eksplicitan sadržaj bez fizičkog čina.
- **Ažurirana informacija iz jula 2024**. **godine**: preko 3.500 novih AI generisanih SIZDM-ova je postavljeno na isti forum, od oktobra 2023. godine (sve češće korišćenje slika poznatih žrtava SZD-a); više slika prikazuje najtežu kategoriju zlostavljanja; video snimci su počeli da kruže (*deepfakes*); upotreba otvorenog/čistog weba za cirkulaciju SIZDM-a se povećava.[16]

Tačke za diskusiju:

- **Tehnološka zloupotreba:** Premda je korisna u mnogim aspektima, vještačka inteligencija može poslužiti za manipulaciju u zlonamjerne svrhe, što predstavlja nove izazove za zaštitu djece.
- **Uticaj na žrtve**: Stvaranje i distribucija sintetičkog SIZDM-a može imati ozbiljne psihološke i socijalne posljedice za žrtve, posebno kada su uključeni vršnjaci.
- **Preventivne mjere:** Potreba za snažnim praćenjem i regulacijom AI tehnologija i online platformi kako bi se spriječile zloupotrebe. Značaj edukacije djece o tome da ne dijele svoje fotografije na internetu (kao i savjetovati roditelje da ne dijele fotografije svoje djece).

Zaključak:

- Ovo pitanje predstavlja primjer mračne strane tehnološkog napretka i hitne potrebe za sveobuhvatnim strategijama za borbu protiv iskorišćavanja djece putem AI.
- Naglasite važnost saradnje između tehnoloških kompanija, organa za sprovođenje zakona i organizacija za zaštitu djece u rješavanju i ublažavanju ovih rizika.

Slajd 43 – Striming uživo seksualnog zlostavljanja djece

Uvod:

- SIZD striming uživo (*prenošenje uživo*) znači da se seksualno zlostavljanje djeteta trenutno prenosi gledaocu na internetu, koji može gledati i/ili se uključiti dok se zlostavljanje događa.
- Prenos uživo je u porastu, posebno u zemljama u razvoju kao što su Filipini ili Madagaskar. Međutim, to se može dogoditi svugdje, a dobrovoljno i indukovano samostalno proizvedeni materijal koji se prenosi uživo su najčešći oblici, dok se žrtve često nalaze u SAD-u i Evropi.

Ključne tačke:

- Postoje 3 vrste takve zloupotrebe[17]: dobrovoljno samo-proizvedeni materijal koji se prenosi uživo (bez prisile), indukovani samo-proizvedeni materijal za prenos uživo (sa prisilom ili mamljenjem), sa distance emitovani materijal (koji daljinski naruči punoljetni gledalac i izvodi druga odrasla osoba – često na svim kontinentima).
- Ne ostavlja trag, osim ako ga neko namjerno ne snimi, što otežava identifikaciju žrtava i počinitelja.
- Izvršioci često posjeduju SIZDM.[18]

Tačka za diskusiju (vježba-ukoliko bude dovoljno vremena)

- Identifikacija djece žrtava prenosa uživo zahtijeva intenzivnu pažnju radi uočavanja znakova SIZDI-a. Koji su to znakovi?

Zaključak:

- Ovaj oblik SIZDI-a pokazuje da tehnološka rješenja samostalno ne mogu uvijek spriječiti ili otkriti takvu zloupotrebu. Stoga interni mehanizmi i procedure za identifikaciju žrtava treba da postave kao priorite izgradnju povjerenja, posmatranje i rad sa djecom.

16 https://www.iwf.org.uk/media/opkpmx5q/iwf-ai-csam-report_update-public-jul24v11.pdf?utm_source=ActiveCampaign&utm_medium=email&utm_content=July%20Newsletter%3A%20Prevention%20and%20emerging%20threats&utm_campaign=July%202024%20Newsletter

Vidi takođe: https://www.aru.ac.uk/news/growing%20demand%20on%20dark%20web%20for%20ai%20abuse%20images

17 https://www.datocms-assets.com/74356/1662373940-netcleanreport-2019.pdf

18 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019

Slajd 44 – Pornografija bez pristanka: Linija za pomoć "Revenge Porn Helpline"

Ovo ne pogađa samo djecu – i odrasli su takođe jako pogođeni.

Pregled sadržaja slajda:

- Istaknite problem dijeljenja intimnih fotografija bez pristanka.
- Naglasite dostupnost podrške za pogođene pojedince.

Napomene izlagača:

Uvod:

- Ovaj slajd se fokusira na Liniju za pomoć "*Revenge Porn Helpline*," iz Ujedinjenog Kraljevstva, koja nudi podršku i savjete pojedincima koji su iskusili dijeljenje intimnih fotografija bez pristanka.
- Iako je naš primarni fokus bezbjednost djece na internetu, ključno je prepoznati da zlostavljanje na internetu pogađa ljude svih uzrasta.

Ključne tačke:

- **Priroda ovog pitanja:**
  - Dijeljenje intimnih fotografija bez pristanka, koje se često naziva "osvetnička pornografija", može uzrokovati značajnu emocionalnu i psihičku štetu.
  - Ova vrsta zlostavljanja nije ograničena na djecu; odrasli se takođe suočavaju sa ovim kršenjima, čime se još više naglašava široki okvir zabrinutosti o bezbjednosti na internetu.
- **Uloga linije za pomoć:**
  - *UK Revenge Porn Helpline* pruža savjete u povjerenju i podršku onima koji su pogođeni.
  - Linija za pomoć pomaže pojedincima da uklone objavljene fotografije bez njihovog pristanka sa interneta i nudi emocionalnu podršku i smjernice o pravnim opcijama.
- **Statistika i uticaj:**
  - Razgovarajte o rasprostranjenosti osvetničkih pornografskih slučajeva, ukoliko su dostupni i rastućoj potrebi za takvim uslugama podrške.
  - Naglasite važnost podizanja svijesti o raspoloživim resursima za pomoć žrtvama ove vrste zlostavljanja.

Tačke za diskusiju:

- Podstaknite učesnike da razmisle o tome kako se mjere sigurnosti na internetu mogu poboljšati da bi se zaštitili od dijeljenja intimnih fotografija bez pristanka.
- Razgovarajte o značaju edukovanja mladih o rizicima i pravnim implikacijama dijeljenja intimnih slika.

Zaključak:

- Zaključite rad potvrđujući značaj sveobuhvatne internet bezbjednosti i sveobuhvatnog seksualnog obrazovanja i dostupnosti resursa podrške za sve starosne grupe.
- Istaknite da se problem ne odnosi samo na djecu, nego i na odrasle osobe, a što zahtijeva širi pristup bezbjednosti na internetu i uslugama podrške.

Slajd 45

Ovaj dijagram predstavlja broj fotografija prijavljenih (i uklonjenih) od strane *Revenge Porn Helpline,* razvrstanih prema polu. U prosjeku, svaki slučaj, koji je primio *Revenge Porn Helpline* od muškarca imao je 0,3 fotografije po slučaju, u poređenju sa 8,6 za žene – što je 30 puta više, prema polu.

Slajd 46 – Uvod u finansijsku iznudu ili 'Sextortion'

- Pređite na sljedeći slajd.

Sliajd 47 – Seksualna iznuda

Uvod u finansijsku iznudu ili 'Sextortion' (Seksualno iznuđivanje)

Definicija:

- **Seksualno iznuđivanje** uključuje prisiljavanje pojedinaca da daju eksplicitne fotografije, video zapise, novac ili druge usluge zbog prijetnji otkrivanja njihovog privatnog sadržaja. Obično počinje interakcijom na internetu, u kojoj je žrtva ubijeđena ili prevarena da podijeli intimni sadržaj, koji se zatim koristi za ucjenu.

Ciljna demografska kategorija

- Iako seksualna iznuda može uticati na svakoga, djeca, mladi i muškarci su posebno ranjivi zbog učestalog korišćenja društvenih medija i internet platformi na kojima mogu postati meta. U 2023. godini, *Revenge Porn Helpline*[19] je izvijestio da je 30% njihovih slučajeva uključivalo seksualnu iznudu, sa ogromnih 93% ovih slučajeva koji su uključivali žrtve muškog pola.

Mehanizmi seksualne iznude:

- **Pribavljanje sadržaja:** Izvršioci dobijaju pristup privatnim slikama ili video zapisima na različite načine, uključujući *hakovanje*, prevaru, lažno predstavljanje ili dijeljenje na osnovu saglasnosti, što se kasnije iskorišćava.
- **Prijetnje i prinuda:** Žrtvama se prijeti objelodanjivanjem njihovog privatnog materijala osim ako se ne povinuju zahtjevima onog koji vrši iznudu, što često dovodi do značajnih finansijskih i emocionalnih patnji.

Uticaj na žrtve:

- **Emocionalne i psihološke patnje**: Žrtve često doživljavaju ozbiljnu anksioznost, strah i stid, što dovodi do dugotrajnih psihičkih problema. Stigma povezana sa seksualnim iznuđivanjem može spriječiti žrtve da potraže pomoć, pogoršavajući njihovu situaciju.
- **Finansijske posljedice**: iznuđivači obično traže novac, što dovodi do finansijskog pritiska, posebno za mlade žrtve ili njihove porodice.

Trend u porastu:

- Primjetan je globalni porast slučajeva seksualnog iznuđivanja, podstaknut široko rasprostranjenom upotrebom tehnologije i internet konekcije. Prijave o seksualnom iznuđivanju značajno su porasle u 2021. godini i to je ostao problem koji je najviše prijavljivan na liniji za pomoć u 2022. godini, naglašavajući stalnu i eskalirajuću prirodu ove prijetnje.

Preventivne mjere i odgovor:

- **Edukacija i svijest**: Ključno je obrazovati mlade ljude o opasnostima dijeljenja eksplicitnog sadržaja i promovirsati sigurna ponašanja na internetu. Otvorena komunikacija između roditelja, vaspitača/nastavnika i djece o bezbjednosti na internetu može pomoći u sprječavanju ovakvih incidenata.
- **Podrška i resursi**: Uspostavljanje sistema podrške, uključujući linije za pomoć, savjetovanje i pravnu pomoć, je od suštinskog značaja. Podsticanje žrtava da prijave seksualnu iznudu putem pristupačnih i anonimnih mehanizama prijavljivanja bez straha od osude ili odmazde je najvažnije za blagovremenu intervenciju.
- Značaj edukacije djece o tome da ne dijele svoje slike na internetu (kao i savjetovati roditelje da ne dijele slike svoje djece).

Zaključak:

- **Poziv na akciju:** Naglasite važnost zajedničkih napora roditelja, vaspitača, ljekara, organa za sprovođenje zakona i tehnoloških kompanija da zaštite pojedince, naročito djecu, od seksualnog iznuđivanja.
- **Dostupni resursi:** Dajte informacije o tome gdje žrtve mogu potražiti pomoć i podršku, naglašavajući značaj anonimnih usluga podrške u rješavanju ovog rastućeg problema.

19 revenge-porn-helpline-report-2023.pdf (revengepornhelpline.org.uk)

Slajd 48 – Porast broja slučajeva seksualne iznude

Uvod u ITV News video o seksualnoj iznudi:

- Sada ćemo gledati kratak informativni snimak (klip) u produkciji *ITV News*-a, u aprilu 2024. godine.[20]
- Ovaj snimak naglašava alarmantne nove brojke o porastu broja žrtava seksualne iznude, posebno usmjerenih na učenike.
- Nudi detaljan prikaz trenutnog pregleda seksualne iznude, fokusirajući se na metode koje izvršioci koriste i uticaj na mlade žrtve.
- Klip takođe sadrži komentare stručnjaka i izvještaje iz stvarnog života, koji naglašavaju ozbiljnost i rasprostranjenost ovog problema.

Ključne tačke na koje treba obratiti pažnju:

- **Statistički porast**: Obratite pažnju na statistiku, koja pokazuje porast prijavljenih slučajeva seksualne iznude.
- **Ciljna demografska kategorija**: Obratite pažnju na specifično ciljanje učenika i razloge koji stoje iza ovog trenda.
- **Ekspertski uvidi:** Poslušajte uvide stručnjaka o tome zašto je seksualna iznuda u porastu i koje mjere se mogu preduzeti za borbu protiv nje.
- **Priče žrtava**: Saslušajte žrtve koje su doživjele seksualnu iznudu, naglašavajući lični uticaj i psihološke posledice.

Slajde 49 – Nacionalno upozorenje: Finansijski motivisana seksualna iznuda

- **Kontekst**: Nacionalna agencija za kriminal (*NCA,* eng.), i Komanda za zaštitu djece od iskorišćavanja na internetu (*CEOP*, eng.) u Ujedinjenom Kraljevstvu izdale su hitno upozorenje obrazovnim ustanovama širom zemlje. Ovo naglašava goruće pitanje seksualne iznude, posebno usmjerene na djecu i mlade ljude.
- **Pregled sadržaja:**
    - **Definicija:** Finansijski (novčano) motivisana seksualna iznuda uključuje prisiljavanje žrtava na plaćanje novca ili ispunjavanje drugih finansijskih zahtjeva pod prijetnjom objavljivanja intimnih fotogrtafija ili video zapisa.
    - **Razmjere problema**: Upozorenje naglašava značajan porast prijavljenih slučajeva širom svijeta, uključujući djecu koja su prisilno dovedena u takve situacije od strane organizovanih kriminalnih grupa (OKG), sa sjedištem u inostranstvu.
    - **Demografija žrtava**: Dok seksualno iznuđivanje pogađa sve uzraste i polove, veliki dio slučajeva uključuje žrtve muškog pola, starosti od 14-18 godina.
- Tačke djelovanja za profesionalce u obrazovnim institucijama:
    - **Steknite razumijevanje**: Upoznajte se sa detaljima finansijski motivisane seksualne iznude čitajući ovo upozorenje i smjernice o dijeljenju golih i polu-golih fotografija, koje je objavio Savjet za internetsku bezbjednost Ujedinjenog Kraljevstva.
    - **Proces upućivanja**: Ako se otkriju ili objave slučajevi seksualne iznude, uputite ih lokalnoj policiji i/ili lokalnim službama za djecu kroz uspostavljene procedure zaštite.
    - **Jezik podrške**: Izbjegavajte korišćenje jezika za osudu žrtava i podržite djecu i mlade u uklanjanju njihovih fotografija.
    - **Osnaživanje:** Edukovati djecu i mlade o tome kako bezbjedno odgovoriti na zahtjeve ili pritiske za pružanje intimnih fotografija ili video zapisa, naglašavajući da odgovornost nije na djetetu.
    - **Važnost svjesnosti:** Ovo upozorenje naglašava važnost budnosti i proaktivnosti u zaštiti djece od rastuće prijetnje seksualne iznude. Od ključnog je značaja da se ove prakse uključe u okvire širih napora za obezbjeđenje bezbjednosti na internetu i zaštite djeteta.

20 'They killed our son': Online scammers tearing families apart as sextortion cases soar | ITV News

Zaključak: Naglasite hitnost i neophodnost kvalitetnog informisanja i potrebu spremnosti za rješavanje slučajeva seksualne iznude u obrazovnim okruženjima. Naglasite ulogu nastavnika u zaštiti djece i njegovanju bezbjednog internet okruženja.

Slajd 50 – Ko su izvršioci?

Napomene izlagača:

Možete početi tako što ćete pitati učesnike: "Šta mislite ko su izvršioci?" Ovo pitanje može pružiti priliku za diskusiju o predrasudama.

Ključne tačke:

- Ne postoji poseban profil izvršilaca krivičnih djela protiv polne slobode na štetu djeteta.
- Zlostavljači mogu biti pedofili, ali ne uvijek. Pedofilija je klinički izraz koji opisuje pojedince koje seksualno privlače djeca pred-pubertetskog uzrasta. Hebefilija se odnosi na one koje privlače djeca u pubertetu (tinejdžeri), na koju mogu uticati mitovi oko *nevinosti*. (*ljekari u sali možda žele da komentarišu ove termine i definicije*) Ovi termini se ne koriste u zakonu; fokus je na kriminalnom ponašanju, a ne na preferencijama pojedinca. Neki izvršioci mogu biti seksualno aktivni samo sa odraslima i zlostavljati djecu jednostavno zato što im se ukazala prilika, ponekad i ne shvatajući da je osoba maloljetna.
- SIZD izvršioci mogu biti i muškarci i žene, iako su pretežno muškarci.
- Oni mogu biti odrasli ili djeca, sa sve većim brojem djece koja se identifikuju kao izvršioci SIZDI-a (pogledajte sljedeće slajdove).
- Na internetu, baš kao i u stvarnom životu, izvršioci su često iz djetetovog okruženja, posebno kada zlostavljanje uključuje samo-generišući materijal[21]: 60% slučajeva zlostavljanja na internetu uključuje izvršioca poznatog djetetu (izvor: Izvještaj *Disrupting Harm*-a[22]).

Tačke za diskusiju:

- Članovi osoblja takođe mogu biti izvršioci SIZDI-a. Koje korake bi preduzeli da otkrijete da li kolega pohranjuje SIZDM na svoje uređaje ili djeci pokazuje pornografski sadržaj?

Slajd 51 – Štetno seksualno ponašanje

U ovom odjeljku razgovaramo o **štetnom seksualnom ponašanju** (*HSB*, eng.) kod djece i mladih u internet okruženju. Razumijevanje HSB-a je ključno, jer obuhvata niz oblika neprikladnog ili uvredljivog ponašanja, koja djeca mogu ispoljiti ili kome mogu biti izložena na internetu. Ovakvi oblici ponašanja mogu imati ozbiljne posljedice na emocionalno i psihičko blagostanje oštećenih pojedinaca.

Ključne tačke za razmatranje:

- **Definicija i opseg: Štetno seksualno ponašanje (HSB):** Odnosi se na oblike seksualnog ponašanja, koje izražavaju djeca i mladi ljudi, koji je neprikladan za njihov razvoj, može biti štetan za njih ili druge, ili biti uvredljiv prema drugom djetetu, mladoj osobi ili odrasloj osobi.
- **Rasprostranjenost:**
  - HSB se sve više prepoznaje u kontekstu digitalnog svijeta, gdje dostupnost i anonimnost na internetu mogu pogoršati ove oblike ponašanja.
  - Studije i izvještaji ukazuju na rastući trend u slučajevima HSB-a među djecom, koji često olakšavaju društveni mediji, aplikacije za razmjenu poruka i platforme za igre na internetu.
- **Faktori koji doprinose HSB-u:**
  - **Izloženost neprikladnom sadržaju**: Djeca mogu oponašati oblike ponašanja kome su bila izložena preko pornografije ili drugog eksplicitnog sadržaja na internetu.
  - **Pritisak vršnjaka i društveni uticaj**: Platforme na internetu mogu pojačati pritisak vršnjaka, što dovodi do normalizacije štetnog ponašanja.

21 https://www.weprotect.org/wp-content/uploads/Global-Threat-Assessment-2023-English.pdf
22 Disrupting Harm | Safe Online

- **Mamljenje**: Izvršioci mogu manipulisati djecom da se izlažu ili učestvuju u HSB-u.

- **Uticaji HSB-a:**
  - **Žrtve:** Djeca, koja su žrtve HSB-a, često doživljavaju dugotrajne emocionalne i psihičke traume.
  - **izvršioci:** Djeca, koja pokazuju HSB ponašanje, mogu se suočiti sa društvenim, obrazovnim i razvojnim izazovima, kao i pravnim posljedicama, i može im biti potrebna specijalizovana podrška za ove oblike ponašanja.
- **Preventivne mjere i odgovori:**
  - **Obrazovanje i svijest:** Učenje djece o zdravim odnosima (posebno o seksualnosti i pristanku) i granicama može pomoći u prevenciji HSB-a.
  - **Kontrole od strane roditelja i staratelja**: Aktivni nadzor i korišćenje roditeljskog nadzora na digitalnim uređajima mogu ublažiti izloženost štetnom sadržaju.
  - **Profesionalna podrška**: Pristup savjetovanju i psihološkoj podršci žrtvama i izvršiocima je od suštinskog značaja.

Nastavljamo sa istraživanjem konkretnih primjera i studija slučajeva, kako bismo razumjeli različite dimenzije HSB-a i kako se one manifestuju na internetu.

Siajd 52 – Svi su pozvani i Ofsted pregled seksualnog zlostavljanja u školama (2021)

Uvod: Ovaj odjeljak se bavi kritičnim pitanjem štetnog seksualnog ponašanja u obrazovnom okruženju, oslanjajući se na dva značajna izvora: platformu *"Svi su pozvani"* i *"Ofsted pregled seksualnog zlostavljanja u školama i fakultetima",* koje su sprovedene 2021. godine[23]. Oba daju značajne uvide i naglašavaju hitnu potrebu za rješavanjem seksualnog uznemiravanja i zlostavljanja kod omladine.

Svi su pozvani (*Everyone's Invited*, eng.):

- **Pregled platforme:**
- **Web stranica:** everyone'sinvited.uk
- **Svrha:** Pokrenuta kako bi se osigurao siguran prostor za osobe koje su preživjele seksualno uznemiravanje i zlostavljanje da anonimno podijele svoja iskustva.
- **Uticaj:** Snažniji odijek glasova hiljada ljudi, otkrivajući rasprostranjenuost ovih problema unutar obrazovnih institucija i šire.
- **Značaj:** Naglašava često neprepoznatu rasprostranjenost seksualnog zlostavljanja i podstiče sistemske promjene u obrazovnom okruženju.

Glavni navodi na slajdu:

- *"Seksualno uznemiravanje i seksualno zlostavljanje na internetu toliko su rasprostranjeni da ih je potrebno rješavati za svu djecu i mlade".*
- ***Tumačenje**: Ovo naglašava rasprostranjenu prirodu seksualnog uznemiravanja i hitnu potrebu za sveobuhvatnim mjerama za njegovo rješavanje.*

***Ofsted* izvještaj o seksualnom zlostavljanju u školama (2021):**

- **Kontekst**: Sprovedeno kao odgovor na svjedočenja podijeljena na platformi *Everyone's Invited.*
- **Opseg**: Opsežan pregled u raznim školama i fakultetima u Ujedinjenom Kraljevstvu.
- **Nalazi:**
  - **Rasprostanjenost:** Seksualno uznemiravanje, uključujući zlostavljanje na internetu, mnogo je češće nego što se to ranije znalo.
  - **Preporuke:**

23 Review of sexual abuse in schools and colleges - GOV.UK (www.gov.uk) [Pregled seksualnog zlostavljanja u školama i fakultetima]

- Škole i fakulteti, zajedno sa multi-institucionalnim partnerima, treba da djeluju proaktivno protiv seksualnog uznemiravanja i zlostavljanja na internetu.
- Djelovanje treba pokrenuti čak i u nedostatku konkretnih izvještaja, priznajući da se takvo ponašanje među učenicima sve više doživljava kao normalno.

- **Značaj**: Pregled naglašava potrebu za proaktivnim mjerama zaštite i važnost stvaranja sigurnog obrazovnog okruženja za sve učenike/studente.

Ključni citati na slajdu:

- *"Preporučuje se da se škole, fakulteti i multi-institucionalni partneri ponašaju kao da se seksualno uznemiravanje i seksualno zlostavljanje na internetu dešavaju, čak i kada nema konkretnih prijava."*
- **Tumačenje:** Ovim se naglašava potreba proaktivnog pristupa u rješavanju problema seksualnog uznemiravanja, uz prihvatanje da nepostojanje prijava ne znači da se incidenti ne dešavaju.

Djeca, a posebno djevojčice, su dobijale često neželjene seksualne fotografije i zahtjeve za intimne fotografije.

Slajdovi 53 do 55 - Uticaj SIZDI-a na žrtve (3 slajda)

Napomene izlagača:

Možete razmisliti o tome da počnete tako što ćete pozvati nekoga u prostoriji da podijeli svoje iskustvo razgovora sa traumatizovanom žrtvom.

Ključne tačke

- SIZDI je traumatizirajuće i može izazvati traumatične i post-traumatske stresne poremećaje, čiji simptomi uključuju: depresiju, anksioznost, neprijateljstvo, pretjerano nepovjerenje, osjećaj krivice, gubitak pamćenja, kao i fizičke simptome (npr. glavobolja, poremećaj ishrane, itd.).
- Ovi simptomi mogu uticati na ponašanje žrtve. On/ona može biti agresivna, odbijati da govori, laže…
- Kontrola izvršioca nad žrtvom takođe može uticati na ponašanje žrtve i njegovu/njenu spremnost da podnese prijavu.
- U takvim slučajevima, ponašanje žrtve može dovesti do pristrasnosti, nesporazuma, sumnji ili iritacije zbog postupanja stručnjaka.
- Ovi simptomi se mogu koristiti kao indikatori SIZDI-ja i mogu pomoći identifikaciji žrtava.

Djelovanje:

- Uticaj SIZDI-a na žrtve se stoga mora uzeti u obzir prilikom rada sa njima. Stručnjaci treba da prepoznaju posljedice traume, iskažu strpljenje, prilagode svoje odgovore djetetu i ponude odgovarajuću podršku (psiho-socijalna i/ili pravna podrška, podrška u uklanjanju njihovih fotografija...).
- Najvažnije: stručnjaci koji rade sa djecom - žrtvama treba da izbjegavaju korišćenje jezika kojim se žrtve okrivljuju, da postavljaju previše pitanja o tome šta se dogodilo, suočavanje sa žrtvom i nasilnikom, komentarisanje ponašanja žrtve ili dovođenje žrtve u opasnost (kao što je kršenje pravila povjerljivost).

Tačke za diskusiju

- Intervjuisanje djece - žrtava seksualnog zlostavljanja zahtijeva posebne vještine. Može se postaviti pitanje učesnicima o njihovoj sposobnosti da vode takve intervjue.

Zaključak:

- Odgovori moraju biti usresređeni na žrtvu i uzeti u obzir sve ove elemente kako bi se izbjegla dalja viktimizacija žrtve.

Ako je moguće (predložena vježba): igra uloga. Jedna osoba (učesnik ili trener) ima ulogu žrtve, koja prijavljuje zlostavljanje (na primjer, distribucija snimljenog seksualnog zlostavljanja koje se prenosi uživo), dok je drugi učesnik profesionalac (socijalni radnik, učitelj ili doktor). Ostali učesnici se mogu podijeliti u 2 grupe: jedna grupa posmatra i zapisuje kako profesionalac razgovara sa žrtvom, dok druga grupa zapisuje predloženi odgovor. Rezultati se takođe mogu koristiti drugog dana kada se raspravlja o politikama i mehanizmima zaštite.

(Ova vježba se može premjestiti na kraj obuke, kao završna vježba. U tom slučaju, treća grupa bi mogla raditi na identifikaciji nedostataka u bezbjednosnim mjerama na internetu).

Slide 56 – Procjena prijetnji alijanse "WeProtect"

Pregled slajda:

- Ovaj slajd pruža sažetak ključnih nalaza o seksualnom iskorišćavanju i zlostavljanju djece na internetu iz procjene prijetnji *WeProtect Globalne alijanse*.
- Naglašava rastući obim i evoluirajuće metode zlostavljanja, naglašavajući potrebu za sveobuhvatnim i koordiniranim odgovorima.

Ključne tačke za razmatranje:

- **Problem koji eskalira:**
  - Seksualno iskorišćavanje djece i zlostavljanje na internetu je sve intenzivnije, kako po obimu, tako i po složenosti.
  - Izvršioci iskorišćavaju nove tehnologije i platforme za ciljanje djece.
- **Važnost bezbjednosti prema dizajnu:**
  - Naglasiti hitnu potrebu za integracijom bezbjednosnih mjera u dizajniranju digitalnih platformi.
  - Razgovarajte o značaju usklađivanja globalnih internet propisa radi stvaranja bezbjednijeg okruženja na internetu.
- **Pristup javnom zdravstvu:**
  - Zagovarati usvajanje strategija u javnom zdravstvu za prevenciju nasilja i zlostavljanja.
  - Uključite mišljenje djece i usvojite pristupe usmjerene na dijete kako biste bolje razumjeli i riješili problem. Pristup fokusiran na žrtve uključuje poštovanje principa "ne nanosi štetu". Stručnjaci bi trebalo da izbjegavaju re-viktimizaciju djece neprikladnim odgovorom (kao što je ranije objašnjeno).
- **Izvršioci su često poznati:**
  - Predstavite statistiku da 60% slučajeva zlostavljanja na internetu uključuje izvršioca poznatog djetetu (izvor: Izvještaj *Disruping Harm*-a[24]).
  - Ovo naglašava važnost edukacije djece o bezbjednim interakcijama na internetu, čak i sa poznatim pojedincima.
- **Brzo mamljenje u okruženju igara:**
  - Podijelite uvid u podatke da je prosječno vrijeme mamljenja (*grooming*) djeteta u okruženju društvenih igara 45 minuta, a u ekstremnim slučajevima se dešava za samo 19 sekundi.
  - Naglasiti potrebu za budnošću i primjenom zaštitnih mjera u okviru društvenih platformi i platformi za igre.

Uvidi koji se mogu primijeniti:

- Podsticati usvajanje proaktivnih sigurnosnih mjera od strane tehnoloških kompanija.
- Promovisati svijest i edukaciju roditelja, vaspitača i djece o rizicima i znacima zlostavljanja na internetu.
- Zagovarati jaču globalnu saradnju i sprovođenje propisa o bezbjednosti na internetu.

Slajd 57 – Uklanjanje slika

Takeitdown.ncmec.org i *stopncii.org* su inicijative osmišljene da pomognu u borbi protiv širenja seksualno eksplicitnih fotografija na internetu, posebno onih koje uključuju maloljetnike ili dijeljenje bez pristanka. U nastavku ispod je sažetak kako svaka platforma radi:

24 Disrupting Harm | Safe Online

TakeItDown (takeitdown.ncmec.org)

Uspostavljen od strane Nacionalnog centra za nestalu i iskorišćavanu djecu (*NCMEC*, eng. skraćenica), *TakeItDown* je posebno namijenjen maloljetnicima koji žele da se eksplicitne fotografije ili video snimci o njima uklone sa interneta. Proces je osmišljen kako bi se sačuvala anonimnost pojedinca.

Kako djeluje:

- **Zahtjev**: Djeca mogu anonimno poslati eksplicitne fotografije ili video zapise platformi *TakeItDown*.
- **Digitalni otisak prsta**: Platforma koristi tehnologiju za kreiranje jedinstvenog digitalnog otiska prsta (*heš* vrijednost) sadržaja, bez pohranjivanja samih slika ili video zapisa.
- **Distribucija baze podataka**: Ovi *hešovi* se dodaju u bazu podataka kojoj mogu pristupiti uključene tehnološke kompanije.
- **Uklanjanje sadržaja**: Kompanije koriste ove *hešove* da identifikuju i uklone sadržaj iz polja svojih usluga, sprječavajući dalje širenje.

StopNCII.org

StopNCII (Intimna slika bez pristanka) je dio *Revenge Porn* linije za pomoć sa sjedištem u Ujedinjenom Kraljevstvu. Kreiran je za žrtve zloupotrebe upotrebe intimne slike bez pristanka, koje su starije od 18 godina.

Kako djeluje:

- **Registracija i verifikacija:** Korisnici se registruju i provjeravaju svoj identitet kako bi bili sigurni da su subjekti predmetnog sadržaja**.**
- **Heš:** Korisnici šalju slike ili video zapise za *heširanje*; stvarni sadržaj se ne pohranjuje.
- **Upotreba heša:** Slično kao *TakeItDown*, ovi *hešovi* se dijele na tehnološkim platformama koje ih koriste za otkrivanje i uklanjanje podudarnog sadržaja.
- **Podrška:** *StopNCII* takođe pruža savjete i podršku žrtvama u rješavanju emocionalnih i pravnih složenosti povezanih sa takvim zlostavljanjem**.**

Sažetak za prezentaciju

Obje platforme koriste tehnologiju *heširanja* kako bi pomogle u uklanjanju eksplicitnog sadržaja sa interneta bez pohranjivanja ili dijeljenja samih slika ili video zapisa. Razlikuju se uglavnom po svojim ciljnim grupama - djeca za *TakeItDown* i odrasli za *StopNCII* - kao i po vrsti podrške koju nude, odražavajući različite pravne i emocionalne potrebe ovih grupa. Ove inicijative predstavljaju moderne, tehnološki vođene pristupe zaštiti digitalnih prava i dostojanstva pojedinaca.

Slajd 58 – Savjet Evrope: Integrisane strategije za zaštitu djece od nasilja

The Council of Europe Policy Guidelines on Integrated National Strategies for the Protection of Children from Violence - Smjernice Savjeta Evrope o integrisanim nacionalnim strategijama za zaštitu djece od nasilja, imaju za cilj da budu izvor inspiracije za države koje teže usvajanju holističkog pristupa nasilju nad djecom i garantovanju djeci djetinjstva bez nasilja. Smjernice sadrže detaljne predloge o tome kako razviti integrisanu nacionalnu strategiju o pravima djeteta i iskorijeniti nasilje nad djecom. Strategija je definisana kao multidisciplinarni i sistematski okvir integrisan u proces nacionalnog planiranja i ukorijenjen u UNCRC, koji okuplja sve zainteresovane aktere.

Cilj: Zaštita djece od svih oblika nasilja, uključujući seksualno zlostavljanje u digitalnom okruženju, kroz integrisani pristup koji naglašava prevenciju, zaštitu, krivično gonjenje i učešće.

Ključne komponente i preporuke:

- **Pravni okvir:**
  - Zalagati se za snažne zakonodavne mjere koje podupiru **Lanzarote konvenciju,** koja je posebno usmjerena na seksualno iskorišćavanje i zlostavljanje djece, osiguravajući stroge, jasne i primjenjive zakone u svim državama članicama.
  - Podsticati zemlje da prilagode svoje nacionalne zakone, kako bi uključili digitalne oblasti u kojima bi djeca mogla biti u opasnosti.
- **Preventivne mjere:**

- Promovisati obrazovne programe i kampanje za podizanje svijesti usmjerene na djecu, roditelje i edukatore, kako bi se povećalo razumijevanje rizika i znakova digitalne eksploatacije.
- Razvijati alate i resurse koji osnažuju djecu da ostanu bezbjedni na internetu.

- **Zaštita i podrška:**
  - Osigurati postojanje djelotvornih sistema za prijavu zlostavljanja i pružanje trenutne, dostupne podrške i usluga savjetovanja djeci - žrtvama.
  - Podsticati razvoj bezbjednog digitalnog okruženja i korišćenje tehnoloških rješenja za otkrivanje i sprječavanje zloupotreba.
- **Krivično gonjenje učinilaca:**
  - Podržati prekograničnu saradnju u procesuiranju krivičnih djela, odražavajući globalnu prirodu interneta.
  - Sarađivati sa pružaocimaa internet usluga i tehnološkim kompanijama, kako bi se osiguralo brzo uklanjanje uvredljivog materijala i traganje za izvršiocima.
- **Učešće djece:**
  - Uključiti stavove i iskustva djece u procese kreiranja politika, kako bi se osiguralo da su mjere relevantne i učinkovite.
  - Promovisati dječje grupe koje zagovaraju i platforme koje omogućavaju djeci da izraze svoje potrebe i predloge za sigurnije digitalne prostore.

Ciljevi ishoda:

- Ojačati kapacitet svih aktera uključenih u zaštitu djece, kako bi se djelotvorno odgovorilo na izazove koje postavlja digitalno okruženje.
- Ostvariti značajno smanjenje incidenata seksualnog zlostavljanja djece na internetu zajedničkim naporima i uz čvrste okvirne politike.

Posvećenost Savjeta Evrope:

- Pokazuje se posvećenost pravima djeteta kroz integraciju standarda zaštite djece u sve aspekte digitalnih politika i praksi, sa ciljem holističkog pristupa koji ne samo da reaguje na prijetnje, već ih aktivno sprječava.

Slajd 59 – Nacionalni aspekti

Elementi o statusu ratifikacije mogu biti uključeni ovdje:

- Crna Gora:

  Lanzarot konvencija: Potpisana 2009. godine, ratifikovana 2010. godine, stupila na snagu 2011. godine.

  CRC Protokol: Sukcesija 2006. godine.

  Crna Gora je preuzela obaveze iz dva Protokola: o oružanim sukobima i o eksploataciji djece, sukcesijom 2006. godine.

6. DOKAZI IZ ISTRAŽIVANJA

Slajd 60 – Dokazi iz istraživanja

Pregled objavljenih akademskih istraživanja (nacionalnih i međunarodnih) o bezbjednosti na internetu.

Slajd 61

Global Kids Online | Children's rights in the digital age[25] Prava djece u digitalnoj eri

- **Istraživačka platforma za dječja iskustva na internetu: *Global Kids Online*** je međunarodna istraživačka inicijativa, koja istražuje dječja iskustva na internetu, rizike i mogućnosti u različitim zemljama i kulturama.
- **Uvidi zasnovani na podacima:** Platforma pruža sveobuhvatne uvide, zasnovane na podacima, koji mogu objezbijediti informacije za politike i prakse, koje imaju za cilj da unaprijede bezbjednost i dobrobit djece u digitalnom svijetu.
- **Saradnja i resursi:** Služi kao prostor za saradnju, nudeći resurse, alate i metodologije za podršku istraživačima, kreatorima politika i praktičarima u razumijevanju i poboljšanju digitalnih života djece na globalnom nivou.

Istraživanje rizika i mogućnosti djece u digitalnom svijetu:[26]

- **Balansiranje rizika i mogućnosti**: Izvještaj istražuje kako digitalne tehnologije predstavljaju i značajne rizike i mogućnosti za djecu, naglašavajući potrebu za zaštitnim mjerama uz maksimiziranje koristi.
- **Nalazi globalnog istraživanja**: Pruža uvide na osnovu globalnog istraživanja o iskustvima djece na internetu, naglašavajući raznolikost načina na koje djeca koriste digitalne platforme i različite uticaje na njihovu dobrobit.
- **Poziv za sveobuhvatne strategije**: Izvještaj poziva na koordinisane napore vlada, tehnoloških kompanija i civilnog društva, kako bi se stvorila bezbjedna i osnažena digitalna okruženja za djecu širom svijeta.

Digital 2024 - We Are Social [27] / Digitalna 2024-Mi smo društveni

- **Prekretnica na društvenim mrežama**: Broj korisnika društvenih medija širom svijeta premašio je 5 milijardi, što predstavlja značajnu prekretnicu u globalnoj digitalnoj povezanosti.
- **Promjena obrazaca upotrebe**: Izveštaj naglašava evoluirajuće trendove u korišćenju društvenih medija, uključujući rastući značaj kratkog video sadržaja i povećan uticaj platformi u nastajanju.

Uvidi u digitalni pejzaž: Analiza pruža ključne uvide u to kako se ljudi bave digitalnim platformama, nudeći vrijedne informacije za preduzeća, marketinške stručnjake i kreatore politika u prilagođavanju digitalnom okruženju koje se brzo mijenja.

---

25 Global Kids Online | Children's rights in the digital age

26 Stoilova, M., Livingstone, S., and Khazbak, R. (2021) Investigating Risks and Opportunities for Children in a Digital World: A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Paper 2020-03. UNICEF Office of Research – Innocenti, Florence.

27 Digital 2024 - We Are Social UK

Slajd 62 – Nacionalno istraživanje i dokazi

- *Global Kids Online* istraživanje: Ovo istraživanje, sprovedeno u saradnji UNICEF-a i Londonske škole ekonomije, pružilo je uvid u ponašanje djece u Crnoj Gori na internetu, uključujući izloženost rizicima kao što su nasilje i neprimjeren sadržaj. Ovo istraživanje je poslužilo kao osnova za kreiranje politika zaštite djece na internetu.[28]
- *Policy Brief* o bezbjednosti na društvenim mrežama: Dokument *DFC Policy Brief* analizirao je izazove u vezi sa zaštitom ličnih podataka i prevencijom sajber kriminala, uključujući prijetnje poput *ransomware* napada i ucjena. Poseban fokus bio je na podizanju svijesti korisnika i jačanju institucionalnog odgovora na digitalne prijetnje.[29]
- Institucija Zaštitnika ljudskih prava i sloboda Crne Gore sprovela je istraživanje o zloupotrebi djece putem interneta. Fokus ovog istraživanja bio je na razumijevanju pojma, rizicima i načinima eksploatacije djece putem informacionih tehnologija. Takođe su analizirani stavovi djece, roditelja i profesionalaca, kao i usklađenost nacionalnog zakonodavstva s međunarodnim standardima. Izvještaj se bavi i praksama kompanija i nevladinog sektora u zaštiti djece na internetu.
- *DoMEn* inicijativa, u saradnji sa partnerima, objavila je edukativni vodič "Bezbjednost djece na internetu i društvenim mrežama". Ovaj vodič pruža informacije o popularnim društvenim mrežama, savjetima za roditeljsku kontrolu i najčešćim rizicima za djecu. Ovi materijali su dio šire strategije za digitalnu edukaciju u Crnoj Gori.[30]

28 https://www.unicef.org/montenegro/media/3106/file/MNE-media-MNEpublication55.pdf
29 https://dfcme.me/wp-content/uploads/DFC_policy-brief_02.pdf
30 https://stemedukacija.me/wp-content/uploads/2022/10/publikacija-bezbjednost-djece.pdf

7. SCENARIJI

Sliajd 63 - Scenariji

Korišćenje scenarija, vježba za diskusiju o implikacijama na djecu i kako odgovoriti na njih.

Slajd 64

- Predstavite ciljeve sesije: razumijevanje složenosti digitalne bezbjednosti i etičkih odgovora.
- Objasnite format: učesnici će biti podijeljeni u tri grupe, a svaka će se baviti jednim od scenarija.
- Ohrabrite kritičko razmišljanje i razmatranje neposrednog i dugoročnog djelovanja u svojim odgovorima.

Scenario br. 1 – Dijeljenje neprikladne slike među vršnjacima

Sažetak scenarija: Djevojčica je poslala svoju golu sliku svom dečku preko *WhatsApp*-a i izgleda da drugi u razredu sada imaju pristup ovoj slici.

Pitanja za diskusiju:

- Koji su neposredni koraci kako bi se osigurali sigurnost i dobrobit djevojčice?
- Kako biste se obratili dečku i drugarima iz razreda koji imaju sliku?
- Koje se preventivne mjere mogu primijeniti kako bi se učenici edukovali o rizicima i posljedicama dijeljenja intimnih slika?

Napomene izlagača:

- Naglasite značaj osjetljivog i povjerljivog pristupa za podršku djevojčici.
- Razgovarajte o pravnim implikacijama, uključujući zakone o zaštiti djece i politike protiv distribucije takvog sadržaja.
- Predložite uključivanje školskih savjetnika i eventualno organa za sprovođenje zakona ako smatrate potrebnim.
- Naglasite obrazovne inicijative poput programa digitalnog građanstva kako biste spriječili takve incidente.
- Podsjetite na potrebu pristupa usmjerenog na žrtve.
- Razgovarajte o tome kako trebalo komunicirati ovaj incident (roditeljima, medijima…).

Scenario br. 2 - Cirkulacija pornografskih slika školskog osoblja

Sažetak scenarija: Prijavljeno je da pornografske slike, koje pripadaju školskom osoblju, kruže među djecom.

Pitanja za diskusiju:

- Koji su koraci za kontrolu širenja ovih slika?
- Kako škola treba da podrži uključene članove osoblja?

- Koje su disciplinske mjere prikladne za učenike koji dijele slike?

Napomene izlagača:

- Naglasite potrebu za hitnom akcijom zaustavljanja dalje cirkulacije (angažovanje IT osoblja, upućivanje učenika da brišu slike, itd.).
- Razgovarajte o mehanizmima podrške za pogođeno osoblje, uključujući pravnu i psihološku pomoć.
- Razmotriti potrebu za jasnom komunikacionom strategijom za borbu protiv glasina i očuvanje dostojanstva svih uključenih strana.
- Razmotrite uključivanje školskih savjetnika za djecu ukoliko smatrate potrebnim.
- Istražite zašto ove slike kruže. Da li ih je osoblje podijelilo s djecom? / i radnje koje treba preduzeti ako je to u pitanju.

Scenario br. 3 – Korišćenje tehnologije nudifikacije

Sažetak scenarija: Dječak je koristio aplikaciju za nudifikaciju kako bi kreirao i dijelio intimne slike djevojčica i podijelio ih sa svojim prijateljima**.**

Pitanja za diskusiju:

- Kako riješiti problem zloupotrebe tehnologije u kreiranju intimnih slika bez pristanka?
- Koje su implikacije za dječaka koji je kreirao i dijelio slike?
- Kako podržati žrtve i odgovoriti na reakciju školske zajednice?

Napomene izlagača:

- Fokusirajte se na ozbiljnu prirodu izrade i distribucije "sintetičkih (*vještačkih*) intimnih slika bez pristanka", naglašavajući pravne posljedice.
- Predložite hitne mjere podrške žrtvama i restorativne prakse ukoliko je odgovarajuće.
- Istaknite potrebu za uvođenjem informacija o novim digitalnim rizicima u školski nastavni plan i program digitalne pismenosti.

Scenario br. 4 - Seksualna iznuda izaziva anksioznost

Sažetak scenarija: Dijete dolazi u vašu ordinaciju žaleći se na probleme sa spavanjem. Tokom konsultacija, otkriva da je žrtva seksualne iznude. Dijete djeluje anksiozno i neodlučno, te nije sigurno šta dalje da uradi. Strahuje da bi eksplicitne slike ili video zapisi mogli biti podijeljeni ako se ne povinuje zahtjevima počinioca.

Pitanja za diskusiju:

1. Koje hitne korake treba da preduzmete kako biste podržali dijete i osigurali njegovu bezbjednost?
2. Na koji način biste osigurali povjerljivost uz uključivanje neophodnih organa zaštite?
3. Koje su odgovarajuće preporuke i prateće akcije za podršku mentalnom zdravlju i dobrobiti djeteta?
4. Kako možete obezbijediti da se dijete osjeća sigurno i podržano tokom ovog procesa?

Napomene izlagača:

- **Neposredna akcija**: Ostanite mirni, slušajte bez osuđivanja, uvjerite dijete i dokumentujte njegovo otkrivanje.
- **Zaštita:** Slijedite protokole zaštite, npr. prijavite službama za zaštitu djece i konsultujte se sa relevantnim vlastima (*nadležnim organima*).
- **Podrška:** Organizujte podršku za mentalno zdravlje i obezbijedite resurse za borbu protiv prijetnji na internetu.
- **Praćenje:** Pratite dobrobit djeteta i održavajte komunikaciju sa timovima za zaštitu, kako biste osigurali stalnu podršku.

Ovaj scenario pomaže zdravstvenim radnicima da razmotre svoju ulogu u zaštiti djece, koja su pogođena iskorišćavanjem na internetu.

Povratne informacije grupe i diskusija

Napomene izlagača:

- Pozovite svaku grupu da predstavi svoja predložena rješenja i obrazloženje.
- Omogućite diskusiju o različitim pristupima i onome što se može naučiti iz svakog scenarija.
- Rezimirajte ključne zaključke i osnažite posvećenost škole sigurnom i pristojnom digitalnom okruženju.

8. TEHNOLOGIJE BUDUĆNOSTI

Slajd 65 – Tehnologije budućnosti

Gledanjem unaprijed, sagledavajući novonastalu tehnologiju, posebno *GenerativeAI* (generativna vještačku inteligenciju) i potencijalne rizike za djecu – šta učesnici treba da razmotre u budućnosti kako bi ih zaštitili?

Slajd 66 – Vještačka inteligencija

- **Šta je generativna vještačka inteligencija (GenAI)?**
  - Definišite *GenAI* (eng. akronim) kao granu vještačke inteligencije koja se fokusira na stvaranje novog sadržaja, u rasponu od teksta i fotografija do zvukova i video zapisa. Koristi naučene obrasce i podatke za generisanje novih i koherentnih rezultata.
  - Naglasite da, za razliku od tradicionalne vještačke inteligencije koja je prvenstveno analitička, *GenAI* je kreativan, čime mu se omogućava da proizvede potpuno nove djelove sadržaja na osnovu njegovih podataka iz obuke.
- **Osnovni mehanizmi generativne vještačke inteligencije:**
  - **Učenje iz podataka**: Objasnite da su GenAI modeli obučavani na velikim skupovima podataka. Ova obuka uključuje pohranu ogromne količine informacija kako bi se razumjele strukture, nijanse i odnosi unutar podataka.
  - **Prepoznavanje obrazaca i predviđanje**: Detaljno opišite kako ovi modeli koriste statističke tehnike za prepoznavanje obrazaca i predviđanje vjerovatnih ishoda. Ova sposobnost je ono što omogućava *GenAI* alatima da generišu sadržaj koji je kontekstualno relevantan i koji se često ne razlikuje od sadržaja koji su stvorili ljudi.
  - **Neuronske mreže**: Uvesti neuronske mreže kao arhitekturu koja se najčešće koristi u GenAI. Oni su inspirisani ljudskim mozgom i dizajnirani da repliciraju njegove sposobnosti prepoznavanja obrazaca. Slojevi čvorova (neuroni) djeluju zajedno kako bi se analizirale ulazne informacije i proizvele izlazne informacije.
- **Primjer *GenAI* djelovanja:**
  - Navedite primjere, koji ilustruju primjenu *GenAI a*plikacija:
    - Modeli generiranja teksta kao što je *GPT* (Generativni unaprijed obučeni transformator) za pomoć pri pisanju.
    - Generatori slika poput *DALL-E,* koji kreiraju slike iz tekstualnih opisa.
    - Sistemi muzičke sinteze koji komponuju muziku zasnovanu na različitim žanrovima i stilovima.

Zaključak:

U zaključku naglasite da *GenAI* predstavlja značajan skok u sposobnostima vještačke inteligencije, prelazeći sa razumijevanja i analize podataka na mogućnost kreativnog generisanja novog sadržaja, koji oponaša ljudski kvalitet i kreativnost.

Ovaj uvod postavlja temelje za razumijevanje osnovne funkcionalnosti i tehnologije koja stoji iza generativne vještačke inteligencije, pružajući jasnu osnovu, prije upuštanja u dublje rasprave o njenim primjenama i etičkim razmatranjima.

Slajd 67 - *ChatGPT*

Prvo pozovite delegate da imenuju logo.

Koliko njih ga je koristilo?

Upoznajte *ChatGPT*: Prekretnicu u konverzacijskoj (razgovornoj) vještačkoj inteligenciji (AI)

Napomene izlagača:

- **Pregled ChatGPT-a:**
  - Definišite *ChatGPT* kao najsavremeniji jezički model koji je razvio *OpenAI,* a koji se zasniva na arhitekturi Generativnog unaprijed obučenog transformatora (GPT).
  - Objasnite da je *ChatGPT* dizajniran za generisanje tekstualnih odgovora nalik ljudima, na nivou konverzacije (razgovora). Može razumjeti i generisati odgovore na osnovu konteksta razgovora, što ga čini vrlo djelotvornim za širok spektar aplikacija, od korisničke službe do kreiranja sadržaja.
- **Razvoj i obuka:**
  - ChatGPT se razvija/obučava korišćenjem varijante mašinskih tehnika učenja poznate kao učenje bez nadzora, gdje se model napaja ogromnom količinom tekstualnih podataka i uči da predvidi sljedeću riječ u rečenici.
  - Proces obuke uključuje prilagođavanje internih parametara, kako bi se minimizirala razlika između predviđenih i stvarnih tekstualnih sekvenci, povećavajući njegovu sposobnost da generiše koherentne i kontekstualno prikladne odgovore.
- **Mogućnosti ChatGPT-a:**
  - Istaknite njegovu kompetetnost u rukovanju različitim temama, od jednostavnih činjeničnih pitanja do složenih diskusija, koje uključuju razmišljanje, savjete i kreativno stvaranje sadržaja.
  - Ukažite na njegovu sposobnost da održi dijalog u nekoliko redova, zapamti kontekst razgovora i pruži odgovore koji su relevantni za kontekst.
- **Navedite primjere:**
  - Ukratko navedite uobičajene slučajeve upotrebe *ChatGPT-a,* uključujući virtualnu pomoć, obrazovne alate, pomoć za kreativno pisanje i još mnogo toga. *ChatGPT* je integrisan u različite potrošačke aplikacije, kako bi se poboljšala interakcija korisnika kroz razumijevanje prirodnog jezika.
  - Iz perspektive SIZDI-a, mogao bi se koristiti za podršku mamljenju djece, kao na primjer:
    - Komanda/prompt: "Pretvori ovu rečenicu na tinejdžerski jezik: "Zdravo, kako si? Da li bi ćaskala/o sa mnom? Koji su tvoji hobiji?"
    - A: "Hej! Šta ima? 'oćeš da ćaskamo? Šta gotiviš ovih dana?»
    - Komanda/prompt: "Pretvori istu rečenicu u jezik za ćaskanje."
    - A: "Hej! kako 'oćeš da ćaskamo? Koje su ti zeze?"
- **Interaktivni segment:**
  - Pozovite učesnike da navedu da li su koristili *ChatGPT,* ili slične alate vođene vještačkom inteligencijom. Ovo može preći u diskusiju o iskustvima iz prve ruke i zapažanjima o tehnologiji.

Zaključak:

- Sumirajte tako što ćete navesti da ChatGPT predstavlja značajan napredak u oblasti vještačke inteligencije, pokazujući potencijal generativnih modela za transformaciju digitalnih interakcija.

Ovaj slajd će pružiti temeljno razumijevanje *ChatGPT*-a, postavljajući temelj za dalje diskusije o njegovim implikacijama i primjenama u različitim sektorima.

Slajd 68 – Sveobuhvatni pregled generativnih AI tehnologija

Naslov: Otkrivanje mogućnosti Generativne AI u raznim medijima.

Napomene izlagača:

- **Generesanje teksta: *ChatGPT, Gemini, Jasper***
  - **ChatGPT:** Koristi mašinsko učenje za simulaciju teksta, sličnog onom koji stvara čovjek, na osnovu komandi/upita, koji je koristan za zadatke, kao što su simulacija razgovora, kreiranje sadržaja i rješavanje problema.
  - **Gemini:** Slično kao u *ChatGPT*-u, Gemini bi mogao biti izmišljeni/fiktivni prikaz alata za generisanje teksta specifičnih za industriju, prikazujući prilagođena rješenja.
  - **Kako to funkcioniše**: Ovi modeli predviđaju vjerovatnoću svake sljedeće riječi na osnovu prethodnih riječi, precizno podešavajući odgovore iz ogromnih skupova podataka teksta.
- **Generisnje slika: DALL-E, MidJourney, Stable Diffusion**
  - **DALL-E:** Generiše slike iz tekstualnih opisa, kreativno mješajući apstraktne koncepte.
  - **MidJourney:** Fokusira se na stvaranje visokokvalitetnih umjetničkih slika za kreativne industrije.
  - **Stable diffusion**: Model dubokog učenja koji omogućava korisnicima da kreiraju detaljne slike iz tekstualnih opisa, dostupne široj publici.
  - **Kako funkcioniše**: Ovi modeli koriste verzije neuronskih mreža koje razumiju i interpoliraju vizuelne podatke, pretvarajući tekstualne opise u složene slike putem naučenih asocijacija.
- **Generisanje video zapisa: Runway SORA, Synthesia, Deepfake Technology**
  - **Runway SORA:** Specijalizovan za uređivanje videa i efekata pomoću vještačke inteligencije.
  - **Synthesia**: Kreira prilagođeni video sadržaj iz teksta, uključujući virtuelne avatare, koji imaju govore ili prezentacije.
  - **Deepfake tehnologija**: Omogućava stvaranje stvarno ubjedljivih video i audio zapisa.
  - **Kako to funkcioniše**: Ove tehnologije analiziraju postojeće video obrasce, kako bi sintetisali novi sadržaj koji odgovara određenim zadatim inputima/parametrima, često koristeći duboko učenje za osiguranje realnosti i koherentnosti.
- **Sinteza glasa: ElevenLabs, Descript's Overdub, Google Duplex**
  - **ElevenLabs*:*** Proizvodi realističan glasovni zvuk (audio) na osnovu teksta.
  - **Descript's *Overdub*:** Omogućava kreiranje prilagođenog govornog sadržaja na osnovu otkucanog teksta.
  - **Kako to funkcioniše:** Modeli sinteze glasa pretvaraju tekst u realističan izgovoreni zvuk, koristeći intonacije i ritmove naučene iz govornih podataka.
- **Generisanje muzike: AIVA, Amper Music, Google Magenta**
  - **AIVA:** Komponuje simfonijsku muziku korišćenjem vještačke inteligencije.
  - **Amper Music:** Omogućava korisnicima da kreiraju zvučne zapise na osnovu zadatih raspoloženja i stilova**.**
  - **Google Magenta:** Istražuje ulogu AI u stvaranju privlačne umjetnosti i muzike.
  - **Kako funkcioniše:** Ovi sistemi analiziraju muzičku teoriju i strukture kako bi komponovali nove muzičke komade, učeći iz ogromnog niza postojećih muzičkih kompozicija.
- **Generisanje koda: GitHub Copilot, Codex by OpenAI**

- **GitHub Copilot:** Pruža predloge koda direktno u IDE-u (integrisani prostor razvoja) na osnovu konteksta korisnika.
- **Codex by OpenA**I: Omogućava prirodni jezik za generisanje koda, pomažući programerima tako što predlaže čitave linije ili blokove koda.
- **Kako to funkcioniše**: Ovi modeli koriste strukturu i sintaksu programskih jezika, predlažući ili generišući isječke koda na osnovu najboljih praksi i naučenih obrazaca.

- **3D Modeling: Runway, NVIDIA's Omniverse, Google Dream Fusion**
  - **Runway:** Nudi kreativne alate za 3D i aplikacije za mašinsko učenje.
  - **NVIDIA-in Omniverse**: Platforma za izgradnju i rad metaverzum aplikacija, uključujući realistične 3D simulacije.
  - **Kako to funkcioniše:** Ovi alati koriste naprednu vještačku inteligenciju za interpretaciju, modeliranje i stvaranje 3D okruženja na osnovu različitih ulaznih podataka (inputa), primjenjujući složene algoritme za simulaciju realističnih tekstura, osvjetljenja i fiziku.

Zaključak:

- Završite tako što ćete naglasiti transformativni potencijal *GenAI*-a u različitim oblastima, omogućavajući kako kreativnost, tako i efikasnost. Naglasite da se ove tehnologije kontinuirano razvijaju, proširujući opseg onoga što se može automatizovati ili poboljšati pomoću AI.

Ovaj slajd pruža prodoran uvod u različite funkcionalnosti i mehanizme koji stoje iza generativne AI tehnologije, demonstrirajući njen uticaj na mnogobrojne medije i industrije.

Slajd 69

Pozovite učesnike da pogledaju ovu savršeno normalnu sliku i vide da li mogu uočiti nešto neobično.

Dama u sredini ima 3 noge. Ruke i prsti izgledaju neobično. Ovo je sintetička slika, nastala u novembru 2023. godine.

Otkrivanje anomalija na sintetičkim slikama

Napomene izlagača:

- **Uvod u anomalije sintetičkih slika:**
  - Objasnite da su anomalije, kao što su nerealne fizičke karakteristike ili nemogući objekti (poput osobe sa tri noge) uobičajene u sintetičkim slikama. Ove anomalije mogu nastati zbog grešaka u razumijevanju ljudske anatomije od strane vještačke inteligencije ili zbog spajanja više slika.
- **Naglasiti specifične anomalije:**
  - Usmjerite pažnju ciljne grupe na anomaliju treće noge na slici. Razgovarajte o tome kako takve greške pružaju jasne dokaze o manipulaciji slikama ili sintetičkom stvaranju.
  - Iskoristite ovu priliku da angažujete publiku, pitajući da li je neko primijetio anomaliju prije nego što je na nju ukazano, podstičući diskusiju o vještinama posmatranja.
- **Tehničko objašnjenje:**
  - Dajte kratko objašnjenje zašto se ove anomalije javljaju, posebno fokusirajući se na ograničenja trenutnih AI tehnologija poput GAN, koje možda ne razumiju savršeno niti mogu da replikuju nijanse ljudskih oblika i prostornih odnosa.
- **Interaktivna analiza:**
  - Podstaknite ciljnu grupu da razmišlja o drugim područjima na slici koja bi mogla izgledati "čudno" ili razgovarajte o tome kako anomalija utiče na ukupnu percepciju autentičnosti slike.
- **Diskusija o etici:**
  - Koristite ovu anomaliju kao odskočnu dasku za raspravu o etičkim implikacijama korišćenja sintetičkih slika. Razgovarajte o mogućnostima zloupotrebe u različitim kontekstima i značaju transparentnosti u medijima.

- **Zaključak:**
    - Sažmite važnost kritičke procjene slika u digitalnom dobu, u kojem sadržaj generisan vještačkom inteligencijom postaje sve češći. Istaknite vještine potrebne za identifikaciju takvih anomalija i etička razmatranja u korišćenju sintetičkih slika.

Slajd 70 – Sora prompt

Sora je OpenAI-ov napredni AI model, koji može generisati realistične video zapise iz tekstualnih komandi/upita. Ovaj model može kreirati složene scene koje odražavaju detaljna uputstva, simulirajući fizički svijet u pokretu. Sora podržava generisanje video zapisa u trajanju do jednog minuta, zadržavajući visok vizuelni kvalitet i tačnost shodno datim upitima. Dizajniran je da razumije i izvede složeno vizuelno pripovijedanje, što ga čini inovativnim alatom za kreativce u različitim poljima, kao što su snimanje filmova i digitalna umjetnost. Trenutno je *Sora* u fazi testiranja, gdje se procjenjuju potencijalni rizici i prostor za poboljšanja**.**

Slajd 71

Primjer iz Sore. Podsjetimo da je ovo potpuno sintetičko. Ova osoba ne postoji i ova lokacija ne postoji. Moguće je identifikovati da je riječ o sintetičkom prikazu – čini se da joj stopala lebde na površini pločnika.

Slajd 72 - GenAI razmatranja

- **Razmatranja o etici:**
    - GenAI izaziva značajnu etičku zabrinutost u vezi sa autonomijom i pravima pojedinaca, posebno kada se koristi u procesima nadzora ili postupcima donošenja odluka kojima nedostaje transparentnost.
    - Kreiranje dubokog lažiranja ili izmanipulisanog sadržaja može dovesti do dezinformacija i uticati na društveno povjerenje, zahtijevajući stroge etičke smjernice za odgovorno upravljanje njegovom upotrebom.
- **Predrasude u AI sistemima:**
    - AI modeli mogu odražavati ili pojačati predrasude prisutne u njihovim podacima iz obuke, što dovodi do diskriminatornih ishoda u oblastima kao što su zapošljavanje, sprovođenje zakona i odobravanje kredita.
    - Rješavanje predrasuda uključuje razlikovanje skupova podataka za obuku i implementaciju fer osviještećnih algoritama, kako bi se osigurao jednak tretman u različitim demografskim kategorijama.
- **Bezbjednosni rizici:**
    - AI sistemi su podložni neprijateljskim napadima gdje blagi, često neprimjetni inputi mogu navesti modele da donesu pogrešne odluke.
    - Sigurnosne mjere moraju uključiti snažnu i kontradiktornu obuku, kontinuirano praćenje i ažuriranje AI sistema za odbranu od takvih prijetnji.
- **AI halucinacije:**
    - AI halucinacije se javljaju kada modeli generišu lažne ili nebitne informacije, što može biti problematično u aplikacijama koje zahtijevaju visoku preciznost, kao što su medicinska dijagnoza ili novinarsko izvještavanje.
    - Strategije za ublažavanje halucinacija uključuju poboljšanje arhitekture modela, fino podešavanje sa preciznim podacima i implementaciju rigoroznih provjera valjanosti.
- **Pitanja plagijata i orginalnosti:**
    - GenAI može replikovati i proizvesti sadržaj koji je veoma sličan postojećim radovima, što predstavlja izazov za autorska prava i originalnost.
    - Razvoj sistema za praćenje porijekla sadržaja generisanog pomoću vještačke inteligencije i integrisanje alata za otkrivanje plagijata su od vitalnog značaja za zadržavanje integriteta i navođenje originalnih kreatora.
- **Kanibalizam podataka:**

- Ovaj fenomen uključuje AI modele koji "gutaju" i preobučavaju svoje rezultate, što potencijalno dovodi do povratnih praznina, koje degradiraju kvalitet proizvedenih informacija.
- Sprječavanje kanibalizma podataka zahtijeva pažljiv dizajn protoka podataka i provjere u cilju osiguranja da rezultati ne utiču rekurzivno na proces obuke bez nadzora.

Zaključak:

Završite isticanjem neophodnosti multidisciplinarnog pristupa u rješavanju ovih izazova, uključujući kreatore politika, tehnologe i stručnjake iz etike, kako bi se osiguralo da se tehnologije GenAI-a razvijaju i primjenjuju na način koji je siguran, pravedan i koristan za društvo.

Slajd 73 - Izvještaj "Online Nation 2023"

Izvještaj Ofcom-a "Online Nation 2023"[31] pruža opsežan pregled digitalnih trendova u Ujedinjenom Kraljevstvu, koji pokriva korišćenje interneta, online platforme i digitalno ponašanje. Istraživanje ispituje način na koji pojedinci i kompanije koriste internet usluge, fokusirajući se na aspekte kao što su korišćenje društvenih medija, navike *striminga*, e-trgovina, digitalno oglašavanje i regulatorno okruženje. Ova analiza naglašava promjene obrazaca u digitalnoj potrošnji i evoluirajuće uloge različitih platformi u svakodnevnom životu. Ovo služi kao korisna tačka poređenja za razumijevanje sličnih trendova u drugim regionima.

Slajd 74

Izveštaj Ofcom-a "*Online Nation 202*3" pruža uvid u upotrebu generativnih sistema vještačke inteligencije među različitim starosnim grupama u Ujedinjenom Kraljevstvu. Evo sažetka ključnih nalaza o tome ko koristi generativne AI sisteme i kako:

- **Primarni korisnici:**
  - **Generacija Z (tinejdžeri i mlađa djeca):** Ova grupa je znatno više angažovana sa generativnim AI tehnologijama u odnosu na druge starosne grupe. Konkretno, 79% online tinejdžera, u dobi od 13-17 godina i 40% mlađe djece, u dobi od 7-12 godina, koristi generativne AI alate.
  - **Odrasli:** Odrasli pokazuju više odbojnosti, pri čemu samo 31% korisnika internet korisnika starosti 16 godina i starijih od 16 godina koristi generativnu vještačku inteligenciju. Među onima koji nisu koristili ove tehnologije, skoro svaka četvrta punoljetna osoba nije svjesna šta je generativna AI.
- **Iskustva korišćenja i primjene:**
  - **Društveno i zabavno**: Najpopularniji generativni AI alat među djecom i tinejdžerima je Snapchat My AI, posebno među tinejdžerkama. Ovaj alat je postao široko dostupan i prvenstveno se koristi za društvene interakcije i zabavu.
  - **Obrazovna i kreativna upotreba**: Generativna *A*I se takođe koristi u obrazovne svrhe, kao što je pomoć u domaćim zadacima, kao i za kreativne zadatke poput pisanja poezije, stvaranja umjetničkih djela, pa čak i kodiranja.
  - **Opšta radoznalost i istraživanje**: Mnogi korisnici, naročito tinejdžeri, istražuju mogućnosti generativne AI iz čiste radoznalosti, što uključuje ćaskanje (chat) sa *A*I, pronalaženje informacija i traženje savjeta.
- **Zabrinutosti i percepcije:**
  - Uprkos visokim stopama upotrebe, postoji snažna svijest o potencijalnim rizicima povezanim sa generativnom vještačkom inteligencijom. Više od polovine korisnika izražava zabrinutost zbog budućeg uticaja na društvo, posebno mlađih korisnika (uzrasta 16-24 godina), koji su ujedno i najproduktivniji korisnici i najviše zabrinuti zbog društvenih implikacija.

Ovi uvidi iz izvještaja *"Online Nation 2023"* ilustruju različite aplikacije i pomiješane percepcije prema generativnoj AI u različitim starosnim demografskim kategorijama, naglašavajući okruženje u kojem su mladi korisnici pioniri, ali i oprezni u pogledu širih implikacija tehnologije.

31 Online Nation 2023 Report (ofcom.org.uk)

Slajd 75

Ovaj slajd predstavlja podatke iz *Ofcom Online Nation izvještaja 2023*, koji se fokusira na korišćenje generativnih *AI* alata od strane korisnika interneta u Ujedinjenom Kraljevstvu, starosti od 16 i više godina. U tabeli je raščlanjen procenat korisnika, koji su koristili različite generativne AI alate, uz dodatnu podjelu između korisnika muškog i ženskog pola.

Ključne tačke:

- **Ukupna upotreba alata generativne AI:**
  - **ChatGPT** je najčešće korišćeni alat generativne vještačke inteligencije, sa **23%** učešća svih korisnika interneta.
  - **Snapchat My AI** slijedi sa **15%**, zatim **Bing Chat** sa **11%**.
  - **DALL-E** i **Google Bard** imaju stopu korišćenja od **9%,** dok **Midjourney** koristi **8%** ispitanika.
- **Rodne razlike u korišćenju alatki vještačke inteligencije:**
  - **ChatGPT** pokazuje najveći disparitet sa **30%** of korisnika muškog pola i **17%** korisnika ženskog pola.
  - **Snapchat My AI** koristi **18%** muškaraca i **12%** žena.
  - **Bing Chat** koristi **15%** muškaraca i **6%** žena.
  - **DALL-E** i **Google Bard** koristi **14%** muškaraca i samo **5%** žena.
  - **Midjourney** koristi **13%** muškaraca i **4%** žena.

Implikacije:

- Podaci ukazuju na značajan rodni jaz u korišćenju generativnih AI alata, pri čemu je veća vjerovatnoća da će muškarci koristiti ove tehnologije nego žene.
- Ovaj trend može ukazati na potrebu za ciljanim obrazovnim inicijativama, kako bi se podstakla balansirana upotreba među polovima.

Tačke za diskusiju:

- **Zašto je ChatGPT vodeći**: Razgovarajte o mogućim razlozima popularnosti ChatGPT-a, kao što su širok opseg primjene i jednostavnost korišćenja.
- **Rodni dispariteti**: Istražite faktore koji doprinose rodnoj praznini u korišćenju alata AI. Razmotrite raspravu o društvenim uticajima, pitanjima pristupačnosti ili različitim interesima za tehnologiju.
- **Budući trendovi:** Nagađajte kako bi se ovi trendovi mogli dalje razvijati. Hoće li se praznina smanjiti kada alati vještačke inteligencije budu više integrisani u svakodnevni život? Na koji način se može osigurati jednak pristup i korišćenje?

Zaključak: Ovi podaci iz izvještaja Ofcom-a naglašavaju trenutne obrasce u usvajanju generativnih AI alata među različitim demografskim kategorijama korisnika. Razumijevanje ovih trendova je ključno za razvoj strategija za promociju ravnopravnog pristupa i korišćenja novih tehnologija.

Slajd 76

Ovaj slajd predstavlja podatke iz ljetnjeg omnibus istraživanja *CHILDWISE iz 2023. godin*[32], naglašavajući korišćenje alata vještačke inteligencije (AI) među djecom na mreži, starosti od 7-17 godina. Slajd detaljno opisuje ukupnu upotrebu i raščlanjuje podatke prema starosnoj grupi i polu.

Ključne tačke:

- **Ukupna upotreba AI alata (starosna dob 7-17):**
  - **59%** djece na internetu je korisitilo najmanje jednu alatku vještačke inteligencije.
  - **Snapchat My AI** je koristilo **51%** djece, što je čini najpopularnijom AI alatkom.
  - **ChatGPT** *je* koristilo **24%** djece.

32 Generative AI in education: Educator and expert views (publishing.service.gov.uk)

- **DALL-E** i **MidJourney** imaju manje procente korišćenja - **7%,** odnosno **6%**,

- **Raščlanjivanje prema starosnoj dobi:**
  - Starosna dob 7-12:
    - **40%** je koristilo neku AI alatku.
    - **30%** koristi *Snapchat My AI*.
    - **12%** koristi *ChatGPT*.
    - **6%** koristi *DALL*-E i **7%** koristi *MidJourney*.
  - Starosna dob 13-17:
    - **79%** koristi neku od AI alatki.
    - **72%** koristi *Snapchat My AI*.
    - **29%** koristi *ChatGPT*.
    - **7%** koristi *DALL-E* i **5%** koristi *MidJourney*.
- **Raščlanjivanje prema polu djeteta:**
  - Dječaci (starosna dob 7-17):
    - **59%** koristilo neku od AI alatki.
    - **48%** koristi *Snapchat My AI*.
    - **14%** koristi *ChatGPT*.
    - **10%** koristi *DALL-E* i **8%** koristi *MidJourney*.
  - Djevojčice (starosna dob 7-17):
    - **59%** koristilo neku od AI alatki.
    - **54%** koristi *Snapchat My AI*.
    - **34%** koristi *ChatGPT*.
    - **4%** koristi *DALL-E* i **4%** koristi *MidJourney*.
- **Detaljan uvid prema polu i starosnoj dobi:**
  - Za djecu starosti od **7-12 godina**:
    - Dječaci: **40%** koristi neku od AI alatki, **28%** koristi *Snapchat My AI*, **9%** koristi *ChatG*PT, **6%** koristi *DALL-E*, **7%** koristi MidJourney.
    - Djevojčice: **39%** koristi neku od AI alatki, **32%** koristi Snapchat My AI, **12%** koristi ChatGPT, **3%** koristi DALL-E, **3%** koristi MidJourney.
  - Za djecu starosti od **13-17 godina**:
    - Dječaci: **78%** koristi neku od AI alatki, **68%** koristi *Snapchat My AI*, **29%** koristi *ChatGPT*, **10%** koristi *DALL-E,* **5%** koristi *MidJourney*.
    - Djevojčice: **80%** koristi neku od AI alatki, **75%** koristi *Snapchat My AI,* **41%** koristi *ChatGPT,* **4%** koristi *DALL-E*, **3%** koristi *MidJourney*.

Implikacije:

- **Visoka uključenost u AI *(vještačku inteligenciju)***: značajan udio djece, posebno tinejdžera, koristi AI alate, naglašavajući njihovu sve veću integraciju u svakodnevne aktivnosti.
- **Rodne razlike**: Postoje značajne razlike u korišćenju AI alata između dječaka i djevojčica, posebno kod alata kao što su ChatGPT i Snapchat My AI.
- **Trendovi vezani za starosnu dob:** Starija djeca (13-17 godina) češće će koristiti AI alate u poređenju sa mlađom djecom (7-12 godina), što sugeriše da se korišćenje AI povećava sa godinama života.

Tačke za diskusiju:

- **Uticaj AI na mlade korisnike**: Razgovarajte o implikacijama rasprostranjene upotrebe AI alata među djecom, uključujući potencijalne koristi i rizike.
- **Obrazovne potrebe**: Naglasite potrebu za obrazovanjem o digitalnoj pismenosti, kako bi osigurali da djeca razumiju kako sigurno i odgovorno koristiti AI alate.
- **Rodni disparitet**: Istražite razloge rodnih razlika u korišćenju AI i kako riješiti ove disparitete.

Zaključak: Podaci iz istraživanja *CHILDWISE* ljetnjeg omnibusa iz 2023. godine, pokazuju da značajan udio djece na internetu koristi AI alate, sa varijacijama između starosnih grupa i polova. Razumijevanje ovih obrazaca upotrebe je od suštinskog značaja za razvoj odgovarajućih obrazovnih odgovora i politike, koji će podržati sigurno i učinkovito korišćenje vještačke inteligencije kod mladih korisnika.

Slajd 77 – Završetak dana 1.

Slajd 78 – Pregled dana 1.

9. BEZBJEDNOSNE STRATEGIJE NA INTERNETU ZA EDUKATORE, SOCIJALNE RADNIKE I DOKTORE

Slajd 79

Detaljna rasprava o tome koje strategije, politike i alate jedna organizacija treba da ima za efikasnu zaštitu djece na internetu.

U zavisnosti od sastava učesnika, mogli bi se grupisati po profesiji.

Slajdi 80 – Pregled strategije za edukatore, doktore i socijalne radnike

Ovaj sveobuhvatni odjeljak ima za cilj opremiti škole, doktore, socijalne radnike i druge stručnjake potrebnim alatima i znanjem za zaštitu mladih u digitalnom dobu. Pokriva ključne aspekte sigurnosti online, uključujući razumijevanje rizika na internetu, implementaciju praktičnih bezbjednosnih strategija i odgovor na incidente. Odjeljak naglašava značaj saradničkih napora između edukatora, roditelja, djece i stručnjaka u stvaranju bezbjednog okruženja na internetu. Pruža izvodljive savjete, preporuke za politike i resurse za promociju odgovornog digitalnog građanstva, kao i zaštitu djece od ugrožavanja na internetu.

Slajd 81 - Autorstvo u online bezbjednosti

Glavne tačke:

- **Saradnički pristup**: Djelotvorne strategije o bezbjednosti na internetu zahtijevaju kolektivne napore različitih grupa stručnjaka, uz obezbjeđenje održivosti i sveobuhvatne ekspertize.
- **Uloga voditelja za sigurnost na internetu**: Iako je imenovanje voditelja za sigurnost na internetu ključno, odgovornost ne može počivati samo na jednom pojedincu. Uspješna strategija mora biti integrisana u cjelokupnu školsku kulturu.
- **Uključivanje mladih**: Angažovanje učenika u razvoju strategije bezbjednosti na internetu je od suštinskog značaja za njenu relevantnost i djelotvornost.
- **Sigurna alatka od 360 stepeni**: Ovaj sistem samo-ocenjivanja pomaže školama da pregledaju i prate svoje politike i prakse bezbjednosti na internetu, i da promovišu saradničke inpute i konstantna poboljšanja.

Diskusija:

- **Prednosti saradnje**: Razgovarajte o tome kako ekstenzivno autorstvo nad strategijom osigurava kontinuitet i široko razumijevanje u cijeloj školskoj zajednici.
- **Angažovanje učenika i roditelja**: Istaknite važnost uključivanja učenika i roditelja u oblikovanje politika bezbjednosti na internetu, kako bi one bile praktične i dobro prihvaćene.
- **Alatke za procjenu**: Uvedite 360 stepeni bezbjednu (safe, eng.) alatku, kao resurs za škole u cilju mjerenja i poboljšanja inicijativa za bezbjednost na internetu.

Zaključak: Stranica naglašava da je holistički i saradnički pristup neophodan za ugrađivanje sigurnosti na internetu u školsku kulturu, vodeći računa da ona ne bude samo učinkovita, već i održiva. Angažovanje svih zainteresovanih aktera, uključujući učenike, roditelje i razne članove osoblja, povećava uticaj i relevantnost strategije.

Slajd 82 – Mehanizmi zaštite i odgovornosti / Rutine izvještavanja

Uvod:

- Uspostaviti jasne interne mehanizme kako bi se osigurale efikasne reakcije na seksualno iskorišćavanje i zlostavljanje djece na internetu (SIZDI). One bi trebalo da uključe sigurne prakse zapošljavanja, procedure izvještavanja, čuvanja dokaza (u skladu sa zakonskim zahtjevima), procese donošenja odluka, komunikaciju koja poštuje privatnost i protokole za odgovore na medijske upite.

Glavne tačke:

- **Pravila o zapošljavanju osoblja:** Sprovedite detaljnu provjeru prošlosti i krivične evidencije za sve zaposlene. Osigurajte da pojedinci sa evidencijom ili sumnjama u vezi sa SIZD-om ne budu zaposleni na pozicijama, koje uključuju rad sa djecom. Strogo pridržavanje ovih pravila pomaže u sprječavanju zapošljavanja pojedinaca, koji mogu predstavljati rizik**.**
- **Aktivno izvještavanje:** Postavite više kanala za prijavljivanje (npr. odrasli od povjerenja, vršnjački mentori, anonimni online obrasci) kako bi djeca i osoblje prijavili svoje probleme, osiguravajući da su dostupni i sigurni.
- **Pasivno izvještavanje:** Pratite diskusije na internetu koje uključuju školu ili organizaciju kako biste rano identifikovali potencijalne probleme. Ovo uključuje praćenje komentara učenika i roditelja.
- **Dosljednost u odgovoru:** Osigurajte da se svi izvještaji obrađuju dosljedno kako bi se održalo povjerenje u sistem. Standardizovana procedura jača pouzdanost i kredibilitet.
- **Očuvanje dokaza:** Sastavite protokole za pažljivo rukovanje digitalnim dokazima kako biste izbjegli promjenu metapodataka. Snimci ekrana (*screenshot*, eng.) su sigurniji od otvaranja datoteka, posebno za SIZDM. Pridržavajte se lokalnih zakona u vezi sa zadržavanjem dokaza, jer osoblje možda nema ovlašćenje da zadrži SIZDM, čak ni zbog prosljeđivanja policiji.
- **Procjena potreba i rizika žrtava:** Procijenite potrebe žrtava i pružite odgovarajuću podršku, baveći se rizicima kao što su odmazda i isključenost. Posavjetujte se sa roditeljima gdje je to prikladno, kako biste osigurali sveobuhvatnu mrežu podrške.

Doprinos nacionalnog konsultanta:

- **Redovna obuka:**
  - Svi zaposleni trebaju proći inicijalnu i kontinuiranu obuku o prepoznavanju i prijavljivanju slučajeva SIZDI-a, te o rukovanju osjetljivim situacijama.
  - Obuke treba uključiti simulacije stvarnih scenarija i uputstva o procedurama.
- **Pristupačne procedure:**
  - Jasno definisati korake prijave za djecu, roditelje i zaposlene (npr. plakati u školama ili brošure s uputstvima).
  - Osigurati da su kanali dostupni na jeziku i načinima prilagođenim uzrastu djece.
- **Standardizovane procedure odgovora:**
  - Svaka prijava treba biti zabilježena, odmah analizirana i proslijeđena nadležnim organima (npr. Policijskoj uparavi, centrima za socijalni rad).
  - Interni tim za reakciju treba procijeniti ozbiljnost prijave i uključiti relevantne službe.
  - U ovim situacijama je potrebno postupati u skladu sa SOP.
- **Proaktivan pristup:** Od izuzetne je važnosti preduzeti mjere prije nego što se nasilje dogodi i to kroz različite edukativne radionice, uključivanje roditelja, razvoj monitoringa (definisanje indikatora uspješnosti kao što je npr. smanjenje broja prijava itd.).

Diskusija:

- **Aktivni kanali za izvještavanje**: Razgovarajte o značaju postojanja različitih i pristupačnih puteva za izvještavanje, kao što su osoblje od povjerenja, anonimni obrasci i vršnjački mentori.

- **Pasivno praćenje**: Istražite kako praćenje raspoloženja na internetu može pomoći u proaktivnom rješavanju problema.
- **Njegovanje povjerenja**: Naglasite potrebu za dosljednim, transparentnim odgovorom na sve izvještaje kako biste izgradili povjerenje.
- **Istrage:** Razgovarajte o prednostima i nedostacima provođenja internih istraga, posebno kada je uključeno osoblje.

Zaključak:

- Uspostavljanje snažnih rutina izvještavanja, kako aktivnih, tako i pasivnih, ključno je za upravljanje bezbjednošću na internetu. Osiguravanje više kanala za izvještavanje i dosljedan odgovor pomaže u održavanju bezbjednog okruženja za učenike i osoblje.

Slajd 83 – Politika bezbjednosti na internetu

Glavne tačke:

- **Stvaranje bezbjednog okruženja**: Djelotvorne politike bezbjednosti na internetu su ključne za njegovanje bezbjednog okruženja sa podrškom za učenike. Ove politike treba da budu jasne, praktične i integrisane u školsku kulturu.
- **Djelotvorna komunikacija**: Politike moraju biti dobro objašnjene/komunicirane, kako bi se osiguralo da ih učenici, roditelji i osoblje razumiju i poštuju. Jasna komunikacija pomaže svima da znaju kako bezbjedno koristiti internet.
- **Jasnoća i razumijevanje**: Djelotvornost politike se može procijeniti tako što će se ispitati učenici, roditelji i osoblje o njihovom razumijevanju pravilnog korišćenja interneta.
- **Redovno preispitivanje**: Politike bezbjednosti na internetu treba redovno revidirati kako bi se pratile brze promjene u tehnologiji, rizicima i ponašanjima.
- **Saradnički pristup**: Kreiranje politike treba da uključi doprinose od strane djece, osoblja i šire školske zajednice, kako bi se osiguralo široko autorstvo i relevantnost.
- **Ključne tačke širenja saznanja**: Važne aspekte politike treba sažeti i integrisati u školsku kulturu kroz različite kanale komunikacije.
- **Politike unakrsnih referenci**: Sigurnost na internetu treba da se navede u srodnim politikama, kao što su ponašanje, crkveno staranje, zdravlje, sigurnost i školski izleti.

Diskusija:

Pitanje za aktivnosti u malim grupama – Da li imate politike bezbjednosti na internetu i da li su uspostavljene politike prihvatljivog korišćenja? Kako znate da su jasne, razumljive i poštovane od strane svih?

- **Osiguravanje djelotvornosti politike**: Razgovarajte o strategijama kako bi se osiguralo da politike sigurnosti na mreži nisu samo sveobuhvatne, već i jasno saopštene i shvaćene od strane svih zainteresovanih strana.
- **Angažovanje školske zajednice**: Istražite načine za uključivanje učenika, roditelja i osoblja u razvoj i širenje politika bezbjednosti na internetu.

Zaključak: Izrada jasnih, dobro komuniciranih i redovno revidiranih politika bezbjednosti na internetu je od suštinskog značaja za podsticanje bezbjednog i korisnog internetskog okruženja. Uključivanjem cijele školske zajednice i integracijom ključnih tačaka u svakodnevni školski život, ove politike mogu djelotvorno podržati pozitivnu i proaktivnu kulturu internet bezbjednosti.

Slajd 84 –Nastavni plan i program za obrazovanje djece

Uvod:

Ovaj slajd se fokusira na značaj integracije sveobuhvatnog obrazovanja o bezbjednosti na internetu u nastavni plan i program, kako bi djeca stekla znanje i vještine za bezbjedno djelovanje u digitalnom okruženju, te da prepoznaju potencijalne rizike i adekvatno odgovore na prijetnje na internetu.

Glavne tačke:

- **Izrada nastavnog plana i programa**: Nastavni plan i program za bezbjednost na internetu treba da bude progresivan, fleksibilan, relevantan i zanimljiv za učenike.
- **Ciljevi nastave**: Fokusirajte se na podučavanje učenika kako da ostanu bezbjedni na internetu, da se zaštite od povreda i preuzmu odgovornost za svoju i tuđu bezbjednost.
- **Izazovi integracije**: Uprkos konkurentnosti drugih oblasti nastavnog plana i programa, od suštinske je važnosti integrisati bezbjednost na internetu, digitalnu pismenost i građansko obrazovanje u postojeće predmete.
- **Okviri i resursi**: Koristite stručne šeme i okvire, kao što je UKCIS okvir "Obrazovanje za povezani svijet", kako biste pomogli u planiranju i implementaciji nastavnog plana i programa.

Diskusija:

Pitanje za aktivnosti u malim grupama – Opišite kako vaše okruženje obrazuje djecu i mlade da steknu znanje, vještine i sposobnosti kada je u pitanju bezbjednost na internetu? Kako ocjenjujete djelotvornost tih nastojanja?

- **Implementacija okvira**: Razgovarajte o tome kako škole mogu koristiti uspostavljene okvire za strukturisanje svog nastavnog plana i programa za bezbjednost na internetu.
- **Strategije integracije**: Istražite praktične načine da uključite teme o bezbjednosti na internetu u gradivo različitih predmeta bez preopterećenja postojećeg nastavnog plana i programa.

Zaključak: Razvijanje sveobuhvatnog nastavnog plana i programa za sigurnost na internetu ključno je za osposobljavanje učenika za bezbjedno kretanje u digitalnom svijetu. Integracijom obrazovanja o bezbjednosti na internetu u različite predmete i korišćenjem već uspostavljenih okvira, škole mogu pružiti zanimljivo i učinkovito iskustvo učenja za učenike.

Slajd 85 – Obrazovanje djece / Primjeri nastavnog plana i programa: UN-ovog ITU Sango resursa za zaštitu djece na internetu

Pregled: *ITU San*go resursi[33] za zaštitu djece na internetu je sveobuhvatan vodič koji je razvila Međunarodna unija za telekomunikacije (ITU) za zaštitu djece u digitalnom svijetu. Bavi se raznim internetskim rizicima i pruža prilagođene smjernice za djecu, roditelje, edukatore, industriju i kreatore politika.

Ključne komponente:

- **Djeca:**
  - **Resursi:** Smjernice za djecu su prilagođene različitim starosnim grupama i sadrže formate prilagođene djeci, kao što su knjige pripovijetki i radne sveske. Ovi resursi imaju za cilj da unaprijede digitalne vještine, promociju sigurnog ponašanja na internetu i osposobljavanje djece da ostvaruju svoja prava na internetu.
  - **Učenje kroz priče**: Sango, maskota zaštite djece na internetu, koristi se za uključivanje mladih učenika pomoću scenarija i pitanja, koja ih uče o pravima i bezbjednosti na internetu.
- **Roditelji i edukatori/vaspitači:**
  - **Smjernice:** Smjernice pomažu roditeljima i nastavnicima da shvate rizike sa kojima se djeca suočavaju na internetu i da stvore sigurno i osnažujuće okruženje. Naglasak je stavljen na otvorenu komunikaciju i stalni dijalog sa djecom o njihovim iskustvima na internetu.
  - **Sistemi podrške**: Preporuke uključuju uspostavljanje sistema podrške kod kuće i u školama kako bi se brzo i djelotvorno riješili problemi bezbjednosti na internetu.

Sugestije za metode edukacije:

- **Obrazovne postavke**: Nastavnici mogu koristiti knjige sa pripovijetkama i radne sveske da edukuju učenike o sigurnosti na mreži na zanimljiv način.
- **Radionice za roditelje**: Škole i društvene organizacije mogu održavati radionice za roditelje koristeći smjernice koje će im pomoći da bolje razumiju i upravljaju aktivnostima svoje djece na internetu.

33 Children | ITU-COP Guidelines (itu-cop-guidelines.com)

Resurs ITU Sango služi kao vitalno sredstvo za različite aktere, pružajući strukturisan pristup zaštiti djece u digitalnom dobu uz promociju njihovih prava i učešća na internetu.

Slajd 86 – Profesionalni razvoj

Ključne tačke:

- **Potrebe za obukom**: Profesionalni razvoj u oblasti bezbjednosti na internetu identifikovan je kao jedna od najslabijih oblasti u školskom obrazovanju.
- **Redovna obuka**: Svo nastavno i nenastavno osoblje treba da prođe redovnu (najmanje jednom godišnje) obuku o bezbjednosti na internetu i odgovoru na SIZDI, a što se može integrisati u širu obuku o zaštiti djece.
- **Revizije vještina**: Sprovedite revizije kako biste procijenili razumijevanje osoblja o bezbjednosti na internetu, osiguravajući da su sposobni za dosljedno prepoznavanje, reagovanje i rješavanje problema sigurnosti na internetu.
- **Napredna obuka**: Neki članovi osoblja bi trebalo da prođu dublju, akreditovanu obuku radi napretka u profesionalnom razvoju u oblasti bezbjednosti na internetu i odgovora na SIZDI.

Diskusija:

Pitanje za aktivnosti malih grupa – Kako osiguravate da svo osoblje dobije odgovarajuću obuku o bezbjednosti na internetu / odgovoru na SIZDI, koja je relevantna i redovno ažurirana?

- **Značaj obuke**: Razgovarajte o neophodnosti stalne obuke, kako bi osoblje bilo u toku sa najnovijim praksama i pitanjima bezbjednosti na internetu.
- **Dosljednost u pristupu**: Istaknite potrebu za jedinstvenim razumijevanjem i pristupom bezbjednosti na internetu svih članova osoblja.
- **Ciljani razvoj**: Istaknite prednosti napredne obuke za određeno osoblje kako biste poboljšali ukupnu sposobnost škole u upravljanju bezbjednošću na internetu.

Zaključak: Ulaganje u redovno i sveobuhvatno stručno usavršavanje svih članova osoblja je ključno za održavanje bezbjednog internet okruženja u školama. Osiguravanjem dosljedne obuke i pružanjem naprednih mogućnosti za određeno osoblje, škole mogu djelotvorno upravljati i ublažiti bezbjednosne rizike na mreži.

Slajd 87 – Bezbjedna infrastruktura

Glavne tačke:

- **Tehnička rješenja**: Sprovođenje tehničkih mjera za zaštitu školskih sistema od eksternih prijetnji i zloupotrebe.
- **Filtriranje**: Škole treba da koriste sisteme filtriranja za upravljanje pristupom sadržaju na internetu, sprječavajući izlaganje nezakonitom ili neprikladnom sadržaju, kao što su slike zlostavljanja dece, pornografija i teroristički materijal.
- **Monitoring**: Djelotvorni sistemi praćenja treba da upozore školu kada dođe do zloupotrebe, podstičući pravovremene intervencije. Ovo je ključni aspekt zaštite.

Diskusija:

- **Balansiranje između bezbjednosti i pristupa**: Razgovarajte o važnosti pronalaska ravnoteže između ograničavanja štetnog sadržaja i omogućavanja obrazovnog pristupa neophodnim resursima.
- **Proaktivno praćenje**: Istaknite potrebu za proaktivnim praćenjem kako bi brzo identifikovali i odgovorili na potencijalne probleme.

Zaključak: Obezbjeđenje sigurne digitalne infrastrukture u školama je od vitalnog značaja za zaštitu učenika. Implementacija robusnog sistema filtriranja i praćenja pomaže u upravljanju pristupom sadržaju na internetu i otkrivanju zloupotrebe, čime se doprinosi sigurnijem internet okruženju za školsku zajednicu.

Slajd 88 - Swiggle.org.uk – Pretraživač na internetu prilagođen djeci

Napomene izlagača:

Uvod u Swiggle:

- Primjer pretraživača prilagođenog djeci – postoje i drugi.
- *Swiggle.org.uk* je pretraživač dizajniran posebno za djecu, pruža sigurno i prilagođeno korisničko iskustvo pretraživanja na internetu.
- Ovaj pretraživač koji je razvio *South West Grid for Learning (SWGfL*), ima za cilj stvaranje bezbjednog okruženja za pretraživanje za mlade korisnike.

Prednosti Swiggle-a:

- **Sigurnosni filteri:**
  - Swiggle koristi napredne sigurnosne filtere za blokiranje neprikladnog sadržaja, osiguravajući da djeca ne budu izložena štetnom materijalu.
  - Pretraživač aktivno filtrira eksplicitne slike, video zapise i web stranice, nudeći bezbrižnost roditeljima i nastavnicima.
- **Fokus na obrazovanju**:
  - Platforma daje prioritet obrazovnom sadržaju, usmjeravajući djecu ka informativnim resursima prilagođenim njihovom uzrastu.
  - Podržava učenje naglašavajući obrazovne web stranice, što ga čini vrijednim alatom za školsku i kućnu upotrebu.
- **Dizajn prilagođen korisniku:**
  - Swiggle ima jednostavan, intuitivan i*nterfejs,* prilagođen dječjim potrebama, što olakšava navigaciju mladim korisnicima.
  - Dizajn uključuje veća dugmad i jasne ikone, olakšavajući privlačno i pristupačno korisničko iskustvo.
- **Podstiče sigurne navike pretraživanja:**
  - Korišćenjemi Swiggle-a, djeca uče da odgovorno pretražuju internet i razvijaju dobre digitalne navike, od malih nogu.
  - Pretraživač takođe pruža savjete i smjernice o bezbjednoj upotrebi interneta, jačajući vještine digitalne pismenosti.
- **Kontrola roditelja i nastavnika:**
  - Swiggle nudi alatke za roditelje i nastavnike za prilagođavanje iskustva pretraživanja, čime je dodat još jedan bezbjednosni nivo.
  - Ove kontrole mogu ograničiti pristup određenim web stranicama i pratiti aktivnost pretraživanja, osiguravajući kontrolisano i sigurno okruženje na internetu.

Zaključak:

- Swiggle.org.uk predstavlja značajan korak za bezbjedno korišćenje interneta za djecu, kombinujući jake bezjednosne mjere sa fokusom na obrazovanje.
- Ohrabrite roditelje i nastavnike da integrišu Swiggle u svakodnevne internet aktivnosti svoje djece, kako bi promovisali bezbjedno i obogaćujuće iskustvo na internetu.

Slajd 89 - TestFiltering.com

Pregled: TestFiltering.com je alat razvijen da pomogne školama, organizacijama i pojedincima u cilju potvrde da njihovi internet filteri učinkovito blokiraju nezakonit, štetan i neprikladan sadržaj. Usluga osigurava usklađenost sa smjernicama i propisima, koji imaju za cilj zaštitu korisnika, posebno djece, od opasnosti na internetu.

Glavne karakteristike:

- **Provjera blokiranja sadržaja**: Platforma testira da li filteri učinkovito blokiraju pristup nezakonitom sadržaju, kao što je materijal za zlostavljanje djece i sadržaj povezan sa terorizmom, kao i neprikladan sadržaj, poput pornografije.
- **Praćenje i izvještavanje**: Korisnici mogu pratiti svoje rezultate testiranja filtera tokom vremena kako bi pratili djelotvornost i konzistentnost svojih sistema za internet filtriranje.
- **Automatizacija sa TestFiltering**+: Ova vrhunska usluga automatizuje proces testiranja na više uređaja, pružajući upozorenja i izveštaje u realnom vremenu. Osigurava kontinuirano praćenje i pomaže u održavanju usklađenosti prema bezbjednosnim standardima.

Primjeri primjene:

- **Škole:** Škole mogu koristiti TestFiltering.com kako bi bile sigurne da njihovi internet filteri štite učenike od štetnog sadržaja, osiguravajući sigurno okruženje za učenje na internetu.
- **Organizacije:** Kompanije i institucije mogu koristiti alat za održavanje bezbjednog pretraživačkog okruženja za svoje zaposlene i korisnike.
- **Roditelji i staratelji**: Pojedinci mogu koristiti uslugu kako bi osigurali da filteri kućnog interneta djelotvorno štite njihovu djecu od pristupa neprikladnom sadržaju.

Prednosti:

- **Jednostavna upotreba**: Usluga je lagana za korišćenje i zahtijeva minimalnu tehničku stručnost za sprovođenje testova i tumačenje rezultata.
- **Proaktivna zaštita**: Automatsko praćenje pomaže u brzom identifikovanju i rješavanju bilo kakvih kvarova u sistemu filtriranja, osiguravajući stalnu zaštitu.
- **Usklađenost:** Pomaže organizacijama i školama da se pridržavaju regulatornih zahtjeva u pogledu bzbjednosti na internetu i filtriranja sadržaja.

Slajd 90 - Evaluacija

Glavne tačke:

- **Prikupljanje povratnih informacija**: Redovno analizirajte mišljenja različitih školskih aktera, uključujući učenike i osoblje, kako biste osigurali da je strategija zaštite na internetu djelotvorna i na pravom putu. Koristite kratke online ankete i alate za prikupljanje uvida.
- **Procjena djelotvornosti**: Procijenite učinkovitost edukacije o sigurnosti na internetu procjenom razumijevanja učenika o ključnim elementima sadržaja učenja. Utvrdite da li učenici cijene obrazovanje koje steknu.
- **Potrebe za usavršavanjem osoblja**: Sprovedite revizije potreba osoblja za obukom, kako biste osigurali da se resursi za profesionalni razvoj djelotvorno koriste i riješili sve nedostatke u znanju ili vještinama u vezi sa bezbjednošću na internetu.
- **Praćenje napretka**: Koristite alate kao što je *360 stepeni* bezbjedni (s*afe, eng.) alat* da biste pratili napredak škole na putu ka poboljšanju bezbjednosti na internetu. Ovaj alat pomaže u mjerenju napretka, informisanju o prilagođavanju strategije i održavanju evidencije o istorijskim poboljšanjima.
- **Promovisanje uspjeha**: Koristite podatke o uspješnim rezultatima za promovisanje bezbjednosti na internetu. Proslavite postignuća i tražite priznanje, kao što je the *Online Safety Mark* (Oznaka sigurnosti na mreži) od 360 stepeni, kako biste prepoznali i potvrdili napore škole.

Diskusija:

- **Mehanizmi povratnih informacija**: Razgovarajte o važnosti stalne povratne informacije od školske zajednice, kako bi se unaprijedila i podesila strategija bezbjednosti na internetu.
- **Mjerenje uticaja**: Istražite metode za mjerenje uticaja edukacije o bezbjednosti na internetu na ponašanje i stavove učenika.
- **Profesionalni razvoj**: Istaknite potrebu za stalnom obukom i razvojem osoblja kako bi mogli odgovoriti bezbjednosnim izazovima na internetu.

Zaključak: Redovna evaluacija strategije bezbjednosti na internetu je od suštinskog značaja za postizanje djelotvornosti i prilagodljivosti. Prikupljanjem povratnih informacija, procjenom obrazovnog uticaja, rješavanjem potreba za obukom osoblja i praćenjem napretka, škole mogu kontinuirano poboljšavati svoj pristup zaštiti učenika u digitalnom okruženju. Promovisanje i proslavljanje uspjeha takođe pomaže u jačanju značaja bezbjednosti na internetu, u okviru školske zajednice.

Slajd 91 – Dan bezbjednijeg interneta (11. februar 2025. godine)

Pregled: Dan bezbjednijeg interneta (*Safer Internet Day - SID*, *eng.*) je godišnji događaj, koji ima za cilj promociju sigurnijeg i odgovornijeg korišćenja internet tehnologije i mobilnih telefona, posebno među djecom i omladinom. Sve je počelo u Evropi 2004. godine, da bi se vremenom počeo proslavljati u više od 100 zemalja širom svijeta. U 2025. godini, proslava će se održati 11. februara.

Mogućnosti predstavljene na Danu bezbjednijeg interneta:

- **Obrazovanje i svijest:**
  - **Škole i nastavnici**: Škole mogu uključiti Dan bezbjednijeg interneta aktivnosti u svoj nastavni plan i program kroz skupove, diskusije u učionici i specijalne projekte, fokusirane na bezbjednost na internetu. Resursi, kao što su planovi lekcija, igre i aktivnosti su dostupni za olakšavanje ovih diskusija.
  - **Roditelji i staratelji**: Roditelji mogu iskoristiti ovaj Dan da se uključe u smislene razgovore sa svojom djecom o bezbjednosti na internetu, koristeći dostupne resurse za vođenje ovih diskusija i jačanje bezbjednog ponašanja na internetu kod kuće.
- **Uključivanje zajednice:**
  - **Radionice i događaji**: Organizacije u zajednice mogu biti domaćini radionica i događaja za edukaciju javnosti o bezbjednim internet praksama. To bi moglo uključivati sesije za različite starosne grupe, od male djece do odraslih, koje se bave specifičnim rizicima na internetu i sigurnosnim mjerama.
  - **Saradnički projekti**: Podstaknite saradnju između škola, lokalnih preduzeća i grupa u zajednici, kako bi se izradili sveobuhvatni programi za bezbjednost na internetu.
- **Industrija i kreatori politika:**
  - **Industrijske inicijative**: Tehnološke kompanije i internet platforme mogu da koriste Dan bezbjednijeg interneta za pokretanje novih bezbjednosnih funkcija, promociju postojećih alata za bezbjedno korišćenje interneta i interakciju sa svojom bazom korisnika, radi isticanja značaja bezbjednosti na internetu.
  - **Zagovaranje politike**: Kreatori politike mogu iskoristiti ovu priliku da uvedu ili pooštre zakonodavstvo, koje ima za cilj zaštitu djece na internetu i promociju digitalne pismenosti.
- **Lični razvoj:**
  - **Pojedinci:** Svako može učestvovati tako što će se edukovati o najnovijim savjetima za bezbjednost na internetu, razmišljajući o svom načinu korišćenja interneta i obavezati se da će internet učiniti bezbjednijim mjestom svojim odgovornim ponašanjem na mreži.
- **Globalno angažovanje:**
  - **Međunarodno učešće**: Dan bezbjednijeg interneta podstiče globalni dijalog o bezbjednosti na internetu, sa događajima i aktivnostima koje ističu kolektivnu odgovornost za stvaranje bezbjednijeg interneta. Na taj način se jača međunarodna saradnja i razmjena najboljih praksi.

Dan bezbjednijeg interneta pruža jedinstvenu priliku pojedincima, školama, organizacijama i kreatorima politika da se okupe i promovišu bezbjedniji digitalni svijet. Koristeći dostupne resurse i aktivnosti, učesnici mogu doprinijeti kulturi bezbjednosti i odgovornosti na internetu (online).

Za detaljnije informacije, resurse i načine uključivanja, možete posjetiti zvaničnu stranicu Dana bezbjednijeg interneta (*Safer Internet Day*).

10. BEZBJEDNOSNE INTERNET STRATEGIJE ZA RODITELJE

Slajd 92

Istraživanje strategija, alata i resursa dostupnih roditeljima da upravljaju upotrebom tehnologije unutar svojih porodica i da stvaraju pravo okruženje. Ovaj dio se fokusira na strategije za uključivanje roditelja kroz prezentacije, pružajući edukatorima/trenerima praktične tehnike da djelotvorno prenesu znanja o bezbjednosnoj praksi na internetu, osnaživanje roditelja da zaštite svoju djecu na internetu i podsticanje saradničkog pristupa digitalnom blagostanju.

Slajd 93

U današnjem svijetu, kojim upravlja digitalizacija, djeca i mladi su povezani više nego ikada prije. Iako internet nudi ogromne mogućnosti za učenje, društvenu interakciju i zabavu, istovremeno izlaže mlade korisnike nizu potencijalnih rizika, uključujući SIZDI (izloženost neprikladnom sadržaju i predatorima na internetu…), sajber maltretiranju, kršenju privatnosti, itd. Za roditelje je od najvećeg značaja da razumiju koncept bezbjednosti na internetu, što će im biti od pomoći prilikom suočavanja sa ovim izazovima i radi zaštite svoje djece od nastanka štete. Poznavajući rizike i bezbjedne prakse na internetu, roditelji se mogu uključiti u otvorene i upućene diskusije sa svojom decom, postaviti odgovarajuće granice i koristiti alate i resurse za stvaranje bezbjednijeg okruženja na internetu. Ovaj proaktivni pristup ne samo da čuva dobrobit djece, već ih takođe osnažuje da koriste digitalne tehnologije odgovorno i samouvjereno.

Ovaj odjeljak uvodi aspekte koje svi roditelji moraju uzeti u obzir. Namijenjen je za korišćenje svim učesnicima obuke koji komuniciraju sa roditeljima kao način za podršku aktivnostima obrazovanja i osnaživanja. Takođe se može poslužiti kao resurs učesnicima za obuku svojih kolega.

Slajd 94 – Poznavanje kućnih uređaja i njihovih pristupnih tački

Uvod: U današnjem digitalnom dobu, domaćinstva su opremljena bezbrojnim povezanim uređajima. Kako bi osigurali učinkovitu sigurnost na internetu, od ključnog je značaja da roditelji imaju sveobuhvatno razumijevanje svih ovih uređaja i njihovih pristupnih tačaka u domaćinstvu. Ovaj odjeljak će vas sprovesti kroz identifikaciju i upravljanje ovim uređajima, od jedne prostorije do druge.

Pregled slajda:

- **Cilj:** Obučite roditelje da prepoznaju sve povezane uređaje u svojoj kući i razumiju njihove pristupne tačke, kako biste poboljšali bezbjednost na internetu.

Ključne tačke:

- **Dnevni boravak:**
  - **Uređaji:** Smart TV, igračke konzole (npr. Xbox, PlayStation), uređaji za striming (npr. Roku, Amazon Fire Stick), pametni zvučnici (npr. Amazon Echo, Google Home) i povezani sigurnosni kućni sistemi.

- **Pristupne tačke**: Ovi uređaji se često povezuju na kućnu Wi-Fi mrežu i mogu ih koristiti više članova porodice, uključujući i djecu.

- **Kiuhinja:**
  - **Uređaji:** Pametni frižideri, pametne pećnice, povezani aparati za kafu i pametni sistemi rasvjete.
  - **Pristupne tačke**: Iako ovi uređaji mogu izgledati bezopasno, oni se često povezuju na internet radi ažuriranja i daljinskog upravljanja, što ih čini potencijalnim ulaznim tačkama za neovlašćeni pristup.
- **Kućna kancelarija:**
  - **Uređaji:** Laptopovi, desktop računari, štampači, skeneri i ruteri.
  - **Pristupne tačke**: Ovi uređaji vjerovatno sadrže osjetljive informacije i imaju direktan pristup internetu. Osiguravanje bezbjednostii ovih uređaja je od ključng značaja za zaštitu ličnih i profesionalnih podataka.
- **Dječje sobe:**
  - **Uređaji:** Tableti, pametni telefoni, laptopovi, igračke konzole i pametne igračke.
  - **Pristupne tačke**: Djeca često koriste ove uređaje za zabavu i obrazovanje. Važno je pratiti njihovu upotrebu i osigurati da postoji kontrola od strane roditelja, kako bi se djeca zaštitila od rizika na internetu.
- **Roditeljske spavaće sobe:**
  - **Uređaji:** pametni telefoni, tableti, pametni televizori i čvorišta pametne kuće.
  - **Pristupne tačke**: Ovi uređaji se koriste za ličnu komunikaciju i zabavu. Uvjerite se da su unesene snažne lozinke i postavke privatnosti.
- **Garaža i vanjski prostor:**
  - **Uređaji:** Povezani sistemi automobila, pametni otvarači garažnih vrata i vanjske sigurnosne kamere.
  - **Pristupne tačke**: Ovi uređaji poboljšavaju udobnost i sigurnost, ali moraju biti osigurani kako bi se spriječio neovlašćeni pristup.

Koraci djelovanja:

- **Inventar**: Izvršite detaljan popis svih povezanih uređaja u svakoj prostoriji. Napravite listu i zabilježite tip uređaja, njegovu lokaciju i njegove primarne korisnike.
- **Sigurnosni pregled**: Provjerite sigurnosna podešavanja svakog uređaja. Osigurajte da imaju jake, jedinstvene lozinke i ažurirani softver.
- **Kontrola pristupa**: Sprovodite roditeljski nadzor i postavite odgovarajuće nivoe pristupa za djecu. Redovno pregledajte i ažurirajte ove postavke.
- **Segmentacija mreže**: Razmislite o postavljanju "mreže za goste" za manje sigurne uređaje i zadržite svoju glavnu mrežu za najvažnije uređaje kao što su kompjuteri i pametni telefoni.

Diskusija:

- Ohrabrite roditelje da podijele svoja iskustva i izazove u upravljanju više povezanih uređaja.
- Razgovarajte o značaju redovnog ažuriranja *firmvera* (komponenta sofvera) radi zaštite od ranjivosti.
- Istražite dostupne alate i resurse za upravljanje i praćenje povezanih uređaja.

Zaključak: Razumijevanjem raznolikosti uređaja u vašem domu i tački pristupa, možete stvoriti bezbjednije digitalno okruženje za svoju porodicu. Redovno pregledavanje i ažuriranje sigurnosnih postavki svakog uređaja proaktivan je korak u zaštiti vašeg domaćinstva od prijetnji na internetu.

Slajd 95 – Razumijevanje korišćenja usluga na kućnim uređajima

Uvod: Nakon identifikacije različitih povezanih uređaja u domaćinstvu, sljedeći ključni korak je razumijevanje usluga kojima se pristupa na ovim uređajima. Ovo pomaže u osiguravanju da roditelji mogu učinkovito pratiti i usmjeravati aktivnosti svoje djece na internetu. Ovaj odjeljak će vas voditi kroz praktičan pristup otkrivanju usluga, koje se koriste na svakom uređaju.

Pregled slajda:

- **Cilj:** Podučite roditelje strategijama za identifikaciju i praćenje internet usluga, koje njihova djeca koriste na različitim uređajima.

Ključne tačke:

- **Početak putovanja:**
  - **Radite sa djecom**: Počnite tako što ćete se baviti svojom djecom. Zamolite ih da vam pokažu aplikacije i *web* stranice, koje često koriste na svakom uređaju. Ovo ne samo da vam pomaže da shvatite njihove navike na internetu, već i otvara dijalog o bezbjednosti na internetu.
- **Popularni servisi koje treba pratiti:**
  - **Društveni mediji**: *Facebook, Instagram, Snapchat, Twitter, TikTok*
  - **Video platforme**: *YouTube, Netflix, Amazon Prime Video*
  - **Igre**: *Xbox Live, Fortnite, Roblox*
  - **Aplikacije za razmjenu poruka**: *WhatsApp, Messenger*
  - **Muzika i zabava**: *Spotify, Apple Music*
  - **Obrazovne aplikacije**: *Google* učionica, *Khan Academy*
  - **Ostalo**: *Pinterest, Google Play Store, App Store*
- **Račun i detalji za prijavu:**
  - **Značaj detalja za prijavu (*login*)**: Razumijevanje usluga koje zahtijevaju informacije za prijavu je ključno. Ovo uključuje poznavanje korisničkih imena i lozinki, te uvođenje roditeljskog nadzora/kontrole, gdje je to moguće.
  - **Postavke privatnosti**: Pregledajte i prilagodite postavke privatnosti za ove usluge, kako biste poboljšali bezbjednost i kontrolu nad informacijama koje se dijele, kao i sa kim se dijele.
- **Regulatorno praćenje:**
  - **Stalni dijalog**: Redovno provjeravajte svoju djecu u vezi njihovog korišćenja ovih usluga. Ohrabrite ih da podijele sa vama sve nove aplikacije ili web stranice koje počnu da koriste.
  - **Dnevnici aktivnosti**: Koristite evidencije aktivnosti uređaja i usluga za praćenje obrazaca njihovog korišćenja. Ovo može pomoći u prepoznavanju bilo kakvog neobičnog ili potencijalno neprimjernog ponašanja.
- **Postavljanje granica:**
  - **Smjernice za korišćenje**: Uspostavite jasne smjernice za korišćenje ovih usluga, uključujući vremenska ograničenja i odgovarajući sadržaj.
  - **Roditeljski nadzor/kontrola**: Koristite ugrađene funkcije roditeljske kontrole na aplikacijama i uređajima da ograničite pristup neprimjerenom sadržaju i upravljate vremenom provedenim ispred ekrana.

Koraci djelovanja:

- **Interaktivna sesija**: Vodite interaktivnu sesiju sa svojom djecom gdje vas oni vode kroz svoje omiljene aplikacije i web stranice. Neka to bude zabavno i edukativno iskustvo.
- **Pregledajte postavke**: Zajedno pregledajte postavke privatnosti i bezbjednosti za svaku uslugu. Objasnite značaj ovih postavki u zaštiti njihovih ličnih podataka.
- **Postavite kontrole**: Postavite roditeljski nadzor na uređajima i uslugama, kako biste osigurali bezbjedno okruženje na internetu.

Diskusija:

- Podijelite iskustva o upravljanju i razumijevanju usluga koje djeca koriste.
- Razgovarajte o izazovima sa kojima se susrećete u praćenju ovih usluga i njihovom prevazilaženju.

Zaključak: Razumijevanje usluga kojima djeca pristupaju na svojim uređajima je ključno za održavanje sigurnog okruženja na internetu. Putem rada sa svojom djecom, redovnog praćenja načina na koji koriste internet i

postavljanja odgovarajućih granica, možete pomoći njihovoj zaštiti od rizika na internetu i promovisati odgovorno digitalno građanstvo.

Slajd 96 – Poznavanje i korišćenje bezbjednosnih kontrola na internetu

Uvod: Ovaj dio se fokusira na upoznavanje roditelja sa osnovnim bezbjednosnim kontrolama na internetu u cilju zaštite njihove djece i porodice. Cijeneći različite nivoe tehničke stručnosti, posebno među roditeljima u Istočnoj Evropi, jasnoća i jednostavnost su najvažniji. Razmotrićemo dijeljenje postavki u porodičnom krugu, kontrolu roditelja, sigurnost lozinke, antivirusni softver i još mnogo toga.

Pregled slajda:

- **Cilj:** Obučite roditelje znanjem i alatima za djelotvorno korišćenje bezbjednosnih kontrola na internetu u cilju stvaranja bezbjednog digitalnog okruženja za njihovu porodicu.

Ključne tačke:

- **Dijeljenje unutar porodice i upravljanje računom (account):**
  - **Funkcije porodičnog dijeljenja**: Objasnite kako funkcioniše porodično dijeljenje na platformama kao što su *Apple* i *Google*. Omogućava roditeljima da dijele aplikacije, muziku i drugo sa svojom djecom dok kontrolišu kakvom sadržaju mogu pristupiti.
  - **Korisnički nalozi**: Ohrabrite roditelje da uspostave individualne korisničke naloge za svakog člana porodice. Ovo omogućava prilagođeni pristup i kontrole za svakog korisnika.
- **Roditeljske kontrole:**
  - **Kontrole na nivou uređaja**: Pokažite kako se uspostavlja roditeljski nadzor na različitim uređajima, uključujući pametne telefone, tablete i igračke konzole. Pokažite gdje se mogu pronaći ove postavke na popularnim uređajima.
  - **Filteri sadržaja**: Razgovarajte o tome kako koristiti filtere sadržaja za blokiranje neprimjerenih web stranica i aplikacija. Navedite primjere usluga, kao što su *YouTube Kids, Netflix* i internet servis provajdera (npr. *BT, Sky, TalkTalk, Virgin Media*).
  - **Ograničavanje vremena provedenog ispred ekrana**: Objasnite kako se postavljaju ograničenja vremena provedenog pred ekranom, kako biste kontrolisati vrijeme tokom kojeg djeca mogu koristiti uređaje svakog dana. Istaknite prednosti balansiranja između aktivnosti na internetu i izvan interneta. (*online i offline*).
- **Bezbjednost lozinke:**
  - **Kreiranje jakih lozinki**: Naglasite značaj upotrebe snažnih, jedinstvenih lozinki za svaki nalog. Dajte savjete o kreiranju složenih lozinki i korišćenju pristupnih fraza (*passphrase*).
  - **Upravitelji lozinki:** Uvedite koncept upravitelja lozinki, koji mogu bezbjedno pohranjivati i generisati lozinke. Preporučite popularne alate poput L*astPass* ili *1Password*.
  - **Dvofaktorska autentifikacija (2FA):** Objasnite šta je 2FA i kako ona dodaje još jedan nivo bezbjednosti. Ohrabrite roditelje da omoguće 2FA na svim važnim računima.
- **Antivirus i bezbjednosni softver:**
  - **Značaj antivirusnog softvera**: Istaknite neophodnost korišćenja antivirusnog softvera za zaštitu uređaja od zlonamjernog softvera i virusa. Preporučite pouzdane antivirusne programe.
  - **Redovna ažuriranja**: Naglasite značaj održavanja svih softvera i operativnih sistema ažuriranim, radi zaštite bezbjednosti od ranjivosti.
  - **Prakse sigurnog pretraživanja**: Ohrabrite korišćenje sigurnih, šifrovanih (enkriptovanih) konekcija (potražite "https://" u URL-u) i sa oprezom ne preuzimajte datoteke, ili ne klikajte na linkove iz nepoznatih izvora.
- **Korišćenje alatki provajdera usluga:**
  - **ISP roditeljski nadzor:** Mnogi provajderi internet usluga nude ugrađeni roditeljski nadzor/kontrolu. Objasnite kako pristupiti i konfigurisati ove postavke putem njihovih web stranica ili korisničke podrške.

- **Postavke sigurnog pretraživanja:** Pokažite kako se omogućavaju funkcije sigurnog pretraživanja na pretraživačima, kao što su *Google* i *Bing,* za filtriranje eksplicitnog sadržaja.

Diskusija:

- Razmijenite iskustva o primjeni i upravljanju bezbjednosnim kontrolama na internetu.
- Razgovarajte o uobičajenim izazovima sa kojima se roditelji suočavaju i praktičnim rješenjima za njihovo prevazilaženje.

Zaključak: Razumijevanjem i korišćenjem različitih dostupnih bezbjednosnih kontrola na internetu, roditelji mogu značajno poboljšati bezbjednost i dobrobit digitalnog okruženja svoje porodice. Redovno pregledavanje i ažuriranje ovih postavki pomoći će djeci da budu bezbjedna dok se kreću kroz svijet interneta.

Slajd 97 – Razumijevanje i upravljanje digitalnim otiskom djece

Uvod: U digitalnom dobu, djeca ostavljaju otisak na internetu pretraživanjem interneta, interakcijama na društvenim mrežama i drugim aktivnostima na internetu. Razumijevanje onoga što djeca traže, koji sadržaj gledaju i šta se o njima govori na internetu, ključno je za njihovu bezbjednost i privatnost. Ovaj odjeljak će vas usmjeriti u pravcu djelotvornog nadzora i upravljanja otiskom vašeg djeteta na internetu.

Pregled slajda:

- **Cilj:** Osposobite roditelje znanjem i alatima za praćenje i upravljanje aktivnostima i prisustvom njihove djece na internetu, kako bi se osigurala njihova sigurnost i privatnost.

Ključne tačke:

- **Razumijevanje digitalnog otiska:**
  - **Istorija pretraživanja:** Objasnite koliko je važno znati šta djeca traže na internetu. Ovo uključuje pretraživače, kao što je *Google* i alternative prilagođene djeci, kao što je *Swiggle*.
  - **Istorija pregledavanja**: Naglasite potrebu za pregledom web stranica i sadržaja koje djeca posjećuju. Ovo pomaže u razumijevanju njihovih interesa i identifikaciji svake potencijalne izloženosti neprimjerenom sadržaju.
- **Prisustvo na društvenim medijima:**
  - **Profili i objave**: Razgovarajte o značaju praćenja dječjih profila na društvenim mrežama, objava i interakcija. Istaknite kako dijeljene informacije mogu biti trajne i vidljive široj publici.
  - **Postavke privatnosti**: Naučite roditelje kako prilagoditi postavke privatnosti na platformama društvenih medija, kako bi kontrolirsali ko može vidjeti objave i lične podatke njihovog djeteta.
- **Reputacija na internetu:**
  - **Digitalni otisak**: Objasnite kako komentari, fotografije i video zapisi objavljeni na internetu doprinose digitalnom otisku djeteta i mogu uticati na njegovu reputaciju.
  - **Potražite njihovo ime**: Ohrabrite roditelje da povremeno pretražuju ime svog djeteta na internetu, kako bi vidjeli koje su informacije javno dostupne i riješili sve nedoumice.
- **Upravljanje otiskom na internetu:**
  - **Redovno praćenje**: Preporučujemo da redovno provjeravate djetetovu istoriju pretraživanja i pregeda. Koristite već ugrađene alatke pretraživača ili softver za roditeljsku kontrolu, kako bi to olakšali.
  - **Obrazovni razgovori**: Uključite se u razgovore sa djecom o značaju njihovog digitalnog otiska i dugoročnim posljedicama njihovih aktivnosti na internetu.
  - **Pozitivan digitalni otisak**: Podstaknite aktivnosti koje doprinose stvaranju pozitivnog otiska na internetu, kao što je stvaranje obrazovnog sadržaja, učešće u pozitivnim online zajednicama i iskazivanje postignuća.

Diskusija:

- Podijelite iskustva o upravljanju dječjim aktivnostima i digitalnim otiskom.

- Razgovarajte o izazovima sa kojima se suočavaju u praćenju i usmjeravanju dječjeg ponašanja na internetu, te praktičnim rješenjima za navedeno.

Zaključak: Razumijevanje i upravljanje digitalnim otiskom djece je od vitalnog značaja za zaštitu njihove privatnosti i ugleda. Redovnim praćenjem njihovih aktivnosti na internetu prilagođavanjem postavki privatnosti i uključivanjem u edukativne razgovore, roditelji mogu pomoći svojoj djeci da se bezbjedno i odgovorno snalaze u digitalnom svijetu.

Slajd 98 – Upoznavanje sa prijavljivanjem problema na internetu

Uvod: Prijavljivanje problema na internetu je ključni korak u održavanju bezbjednog digitalnog okruženja. Roditelji i djeca bi trebalo da budu svjesni kako se prijavljuje štetan sadržaj, sajber maltretiranje i drugi bezbjednosni problemi na internetu. Ovaj odjeljak će vas uputiti na proces prijavljivanja problema na različitim platformama i naglasiti ključne organizacije koje podržavaju bezbjednost na internetu.

Pregled slajda:

- **Cilj:** Prenesite roditeljima znanje i resurse za učinkovito prijavljivanje štetnog sadržaja na internetu, osiguravajući brzu akciju i rješenje.

Ključne tačke:

- Prijavljivanje putem specifičnih platformi:
  - **Platforme društvenih medija**: Svaka platforma društvenih medija ima svoje mehanizme prijavljivanja. Upoznajte se sa procesima kod popularnih platformi:
    - ***Facebook*:** Koristite dugme "Report" (*prijavi*) kod objava, profila, ili komentara da prijavite neprimjeren sadržaj.
    - **Instagram:** Kliknite na tri tačkice kod objave ili profila i izaberite "Report" (*prijavi*) da bi označili sadržaj ili račune (*account*, eng.).
    - **X/Twitter:** Kliknite na donju strelicu ili tri tačkice na tvitu, potom izabrite "Prijavi tvit", kako bi prijavili tvit sa štetnim sadržajem.
    - **YouTube:** Kliknite na tri tačkice ispod videa, potom izaberite "Report" (*prijavi*) da bi označili neprikladne video snimke.
  - **Usluge igara i striminga**: Razumijevanje alata za prijave u oblasti usluga za igre, kao što *je Xbox Live* i platformama za striming kao što su *Twitch* i *Netflix*.
- **Ključne organizacije:**
  - **Sektor za informatički kriminalitet (Policija Crne Gore):** Policija ima posebnu jedinicu koja se bavi prijavama zlostavljanja na internetu, posebno seksualnog zlostavljanja i iskorišćavanja djece. Ovdje se mogu prijaviti ozbiljni slučajevi kriminala, a takođe postoji i podrška za žrtve.
  - **Nacionalni CIRT:** Nacionalni tim za sajber incidentne odgovore prati i reaguje na sajber prijetnje, uključujući prijetnje koje targetiraju djecu i omladinu.[34]
  - **Zaštitnik ljudskih prava i sloboda Crne Gore:** Mogućnost *onlajn* prijavljivanja posredstvom „hrabrog sandučeta" koje predstavlja brz je efikasan način prijavljivanja zloupotreba djece putem interneta. Ova platforma direktno je povezana sa Vladinim tijelom CIRT, namjenjenom upravo zaštiti djece od svih štetnih sadržaja putem interneta.[35]
  - ***Internet Watch Foundation* (IWF):** Fokusira se na uklanjanje sadržaja seksualnog zlostavljanja djece sa interneta. Prijave se mogu podnijeti direktno preko njihove web stranice.
  - ***True Vision*:** Pruža informacije o krivičnim djelima iz mržnje i alatkama za prijavljivanje na internetu.
  - ***Action Fraud*:** Nacionalni centar za izvještavanje o prevarama i računarskom kriminalu u Ujedinjenom Kraljevstvu pruža platformu za prijavu prevara i obmana putem interneta.
- **Koraci u prijavljivanju:**

34 https://www.gov.me/cirt
35 https://www.ombudsman.co.me/djeca/siguraninternet.html

- **Identifikujte problem**: Shvatite vrstu sadržaja ili ponašanja koje treba prijaviti.
- **Koristite alate za platformu**: Koristite ugrađene alate za prijavljivanje na platformi na kojoj se ovo pitanje pojavi.
- **Potražite podršku**: Kontaktirajte relevantne organizacije za smjernice i podršku, ako je potrebno.
- **Praćenje:** Pratite situaciju i osigurajte da platforma ili organizacija adekvatno riješi problem.

Koraci djelovanja:

- **Interaktivna demonstracija:** Izvedite uživo demonstraciju prijavljivanja problema na popularnim platformama društvenih medija i uslugama za igre.

Diskusija:

- Podijelite iskustva o prijavljivanju problema na internetu i primljenim odgovorima.
- Razgovarajte o izazovima sa kojima se suočavamo u izvještavanju i kako ih prevazići.

Zaključak: Razumijevanje postupka prijavljivanja problema na internetu je ključno za održavanje sigurnog digitalnog okruženja. Upoznavanjem sa mehanizmima prijavljivanja i ključnim organizacijama, roditelji se mogu uspješno riješiti izazove štetnog sadržaja i zaštititi svoju djecu na internetu**.**

Slajd 99 – Roditelji kao uzori za ponašanje na internetu

Uvod: Djeca često oponašaju ponašanja koja primjećuju kod svojih roditelja. Kao digitalni uzori, roditelji igraju ključnu ulogu u oblikovanju navika i stavova svoje djece na internetu. Ovaj odjeljak će pobuditi razmišljanje i diskusiju o tome kako ponašanje roditelja na internetu utiče na njihovu djecu i pružiti praktične strategije za podsticanje pozitivnog digitalnog građanstva.

Pregled slajda:

- **Cilj:** Ohrabrite roditelje da razmisle o svom ponašanju na internetu i da shvate značaj modeliranja pozitivnih digitalnih navika za svoju djecu.

Ključne tačke:

- **Djeca oponašaju roditeljsko ponašanje:**
  - **Opservacijsko učenje:** Objasnite kako djeca uče ponašanje posmatrajući odrasle. Istaknite značaj djelovanja roditelja na internetu, kao primjera za njihovu djecu.
  - **Dosljednost:** Naglasite potrebu za dosljednošću u ponašanju na internetu i izvan njega, kako biste ojačali pozitivne navike.
- **Pozitivno digitalno građanstvo:**
  - **Poštovanje i ljubaznost**: Ohrabrite roditelje da pokažu poštovanje i ljubaznost tokom interakcije na internetu. Pokažite kako ovakva ponašanja postavljaju standarde za djecu.
  - **Privatnost i sigurnost**: Razgovarajte o značaju postavljanja primjera dobrih praksi u pogledu privatnosti i sigurnosti, kao što je korišćenje jakih lozinki i oprez u dijeljenju ličnih podataka.
- **Upravljanje vremenom ispred ekrana:**
  - **Uravnotežena upotreba**: Zagovarajte balans u provođenju vremena ispred ekrana. Roditelji treba da pokažu da su digitalni uređaji alati za učenje i zabavu, a ne da odvlače pažnju od stvarnih interakcija u životu.
  - **Kvalitetan sadržaj**: Predložite roditeljima da dijele visokokvalitetne i obrazovne sadržaje sa svojom djecom, kako bi promovisali produktivno provedeno vrijeme ispred ekrana.
- **Otvorena komunikacija:**
  - **Razgovaranje o iskustvima na internetu**: Ohrabrite roditelje da otvoreno govore o svojim iskustvima na internetu, uključujući izazove i pozitivne interakcije. To podstiče kulturu transparentnosti i povjerenja.
  - **Aktivno slušanje**: Istaknite značaj slušanja o dječjim brigama i iskustvima na internetu, iskazujući empatiju i podršku.

- **Postavljanje granica:**
    - **Digitalne granice**: Roditelji bi trebalo da uspostave i pridržavaju se digitalnih granica, kao što je odsustvo uređaja za stolom tokom obroka, ili u toku porodičnog druženja, kako bi promovisali zdrave digitalne navike.
    - **Granice modeliranja uloga**: Kada roditelji poštuju svoje vlastite granice, veća je vjerovatnoća da će djeca slijediti njihov primjer.

Koraci djelovanja:

- **Vježba samo-refleksije**: Zamolite roditelje da razmisle o svom ponašanju na internetu, kao i da identifikuju oblasti u kojima mogu biti bolji, kako bi pružili bolji primjer.
- **Interaktivna diskusija**: Omogućite diskusiju o uobičajenim oblicima ponašanja na internetu i kako oni utiču na djecu. Podijelite iskustva i strategije za poboljšanje.

Diskusija:

- Podijelite priče i iskustva o tome kako je ponašanje roditelja na internetu uticalo na djecu.
- Razgovarajte o zajedničkim izazovima u postavljanju pozitivnog ponašanja na internetu i zajedno promišljajte o rješenjima.

Zaključak: Kao digitalni uzori, roditelji imaju dubok uticaj na ponašanje njihove djece na internetu i njihove stavove. Pokazivanjem poštovanja, odgovornosti i balansa u korišćenju interneta, roditelji mogu pomoći svojoj djeci da se razviju u pozitivne digitalne građane.

Slide 100 - Upravljanje vremenom isped ekrana – Smjernice Glavnih ljekara Ujedinjenog Kraljevstva

Uvod: Upravljanje vremenom ispred ekrana je značajan izazov za mnoge roditelje. Glavni medicinski stručnjaci Ujedinjenog Kraljevstva dali su praktične savjete kako bi pomogli roditeljima da uravnoteže prednosti i negativne efekte aktivnosti pored ekrana na mentalno zdravlje i dobrobit djece. Ovaj odeljak će izložiti ključne preporuke i strategije za efikasno upravljanje vremenom ispred ekrana.

Pregled slajda:

- **Cilj:** Pružiti roditeljima korisne savjete i strategije za upravljanje vremenom koje njihova djeca provode ispred ekrana na osnovu preporuka glavnih medicinskih stručnjaka Ujedinjenog Kraljevstva.

Ključne tačke:

- **Pristup iz predostrožnosti:**
    - **Balansirajte prednosti i rizike**: Naglasite značaj ravnoteže između prednosti korišćenja ekrana, kao što su obrazovni sadržaj i društvena povezanost sa potencijalnim negativnim efektima, poput smanjene fizičke aktivnosti i poremećaja sna.
- **Vrijeme za obrok bez gledanja u ekran:**
    - **Interakcija oči u oči**: Podstaknite vrijeme za obrok bez ekrana kako biste promovisali razgovore oči u oči i porodično zbližavanje. Istaknite značaj posvećivanja pune pažnje sagovornicima tokom obroka.
- **Bez gledanja u ekran prije odlaska u krevet:**
    - **Higijena spavanja**: Preporučite držanje ekrana izvan spavaće sobe i izbjegavanje korišćenja ekrana prije spavanja, kako biste poboljšali kvalitet sna. Objasnite kako plavo svjetlo sa ekrana može ometati tjelesni ciklus spavanja i buđenja.
- **Pravite redovne pause:**
    - **Pravilo dva sata:** Savjetujte da se prave pauze nakon dva sata neprekidnog korišćenja ekrana kako biste spriječili naprezanje očiju i promovisali fizičku aktivnost. Ohrabrite roditelje da postave tajmere ili koriste aplikacije koje podsjećaju djecu da prave pauze.
- **Dogovor o postavljanju granica:**

- **Postavljanje ograničenja**: Razgovarajte sa djecom o značaju postavljanja i dogovaranja vremenskih ograničenja ispred ekrana i smjernica za ponašanje na internetu. Uključite djecu u kreiranje ovih pravila kako biste bili sigurni da ih razumiju i poštuju.

- **Vodite primjerom:**
  - **Modeliranje ponašanja**: Istaknite ulogu roditelja kao uzora u upravljanju vlastitim vremenom ispred ekrana. Pokažite djeci kako da balansiraju korišćenje ekrana sa drugim aktivnostima, tako što ćete sami upražnjavati dobre prakse.
- **Otvorena diskusija:**
  - **Porodični razgovori**: Ohrabrite obične porodične rasprave o vremenu provedenom ispred ekrana. Postavljajte pitanja, poput: "Da li je vrijeme naše porodice pred ekranom pod kontrolom?" i "Da li ekrani ometaju naš san ili porodično druženje?" da bi procijenilii i prilagodili navike ispred ekrana saglasno potrebi.

Koraci djelovanja:

- **Interaktivna vježba**: Izvedite vježbu u kojoj roditelji opisuju svoje trenutne navike o vremenu koje provode ispred ekrana i da odrede gdje je moguće napraviti poboljšanje. Navedite obrazac za postavljanje pravila i vremenska ograničenja.
- **Materijali za dijeljenje**: Podijelite materijale sa smjernicama i savjetima glavnih medicinskih stručnjaka Ujedinjenog Kraljevstva za upravljanje vremenom ispred ekrana. Uključite praktične korake i alate za njihovu implementaciju.
- **Sesija pitanja i odgovora**: Opredijelite vrijeme za roditelje da postavljaju pitanja i podijele svoja iskustva u vezi upravljanja vremenom ispred ekrana. Ponudite personalizovane savjete na osnovu specifičnih izazova sa kojima se susrijeću.

Diskusija:

- Podijelite uspješne priče porodica koje su primjenile ove smjernice i ostvarile pozitivne rezultate.
- Razgovarajte o uobičajenim izazovima u smanjivanju vremena provedenog ispred ekrana i promišljajte o rješenjima na nivou grupe.

Zaključak: Djelotvorno upravljanje vremenom ispred ekrana ključno je za održavanje mentalnog zdravlja i dobrobit djece. Usvajanjem smjernica glavnih medicinskih stručnjaka Ujedinjenog Kraljevstva i uključivanjem djece u postavljanje granica, roditelji mogu stvoriti uravnoteženo i zdravo digitalno okruženje kod kuće.

Slajd 101 - Kiko and the Manymes

1. **Pregled resursa**:
   - "*Kiko and the Manymes*"[36] je edukativni strip koji je izdao Savjet Evrope sa ciljem podučavanja djece o konceptima digitalnog identiteta i bezbjednosti na mreži.
   - Pustite video u *PowerPoint*-u.
   - Priča prati mladog lika po imenu Kiko, koji se kreće kroz različite scenarije na internetu, pomažući čitaocima da shvate značaj upravljanja svojim digitalnim otiscima i identitetima.
2. **Ključne teme i poruke:**
   - **Svijest o digitalnom identitetu**: Strip naglašava kako radnje preduzete na internetu doprinose digitalnom identitetu osobe i donose potencijalne dugoročne implikacije.
   - **Privatnost i zaštita podataka**: Naglašava značaj zaštite ličnih podataka i opreza u pogledu sadržaja koji se dijeli na internetu.
   - **Kritičko razmišljanje**: Podstiče djecu da kritički razmišljaju o informacijama sa kojima se susrijeću na internetu i o ličnostima koje oni ili drugi predstavljaju.
3. **Upotreba u obrazovnom okruženju:**

36 https://www.coe.int/en/web/children/kiko-and-the-manymes

- Ovaj resurs služi kao početak razgovora za vaspitače i roditelje o temama bezbjednosti na internetu sa djecom, na privlačan i njima blizak način.
- Može se integrisati u lekcije o pismenosti na internetu, građanskom obrazovanju ili ličnom razvoju.

4. **Aktivnosti za podršku**:
   - Pored stripa, dodatno mogu postojati i prateći materijali, kao što su vodiči za diskusiju, aktivnosti ili pitanja kako bi se utvrdile naučene lekcije i olakšalo dublje razumijevanje.
5. **Pristup i distribucija:**
   - Strip je dostupan na više jezika i može mu se pristupiti besplatno putem datog linka, što ga čini raznovrsnim alatom za različita obrazovna okruženja.
6. **Važnost resursa:**
   - Imajući u vidu sve veći digitalni angažman djece, resursi poput "*Kiko and the Manymes*" su od vitalnog značaja za sticanje znanja i vještina za mlade korisnike, u cilju njihovog bezbjednog i odgovornog kretanja u prostoru interneta.

Preporuka: Ohrabrite nastavnike i roditelje da koriste ovaj strip kao dio svog alata za podučavanje digitalnog građanstva i za podsticaj otvorenih diskusija sa djecom o njihovom iskustvu na internetu.

11. POSTOJEĆA PRAKSA

Slajd 102

Prilika da razmotrite i podijelite među učesnicima postojeće mjere i praksu bezbjednosti na internetu. Na sesiji će se utvrditi primjeri dobre prakse.

U zavisnosti od sastava učesnika, mogli bi se grupisati prema profesiji.

Slajd 103 - Olakšavanje diskusije o postojećim praksama za zaštitu djece

Uvod: U sljedećem dijelu ćemo stvoriti prostor za učesnike, uključujući nastavnike, doktore i socijalne radnike, da podijele svoje sadašnje prakse za zaštitu djece na internetu i izvan interneta. Ova diskusija ima za cilj stimulisanje saradničkog okruženja, u kojem profesionalci mogu učiti iz međusobnih iskustava i strategija.

Pregled slajda:

- **Cilj:** Podstaknite učesnike da podijele svoje prakse, razgovaraju o izazovima i uče iz međusobnih iskustava kako bi poboljšali napore u zaštiti djece, sa fokusom na SIZDI.

Ključne tačke:

- **Priprema za diskusiju:**
  - **Svrha:** Objasnite da je svrha ove diskusije razmjena djelotvornih praksi i strategija za zaštitu djece u različitim okruženjima, uključujući škole, zdravstvene ustanove i socijalne službe.
  - **Bezbjedan prostor**: Naglasite značaj stvaranja sigurnog prostora bez osuđivanja, u kojem se svi osjećaju ugodno dijeleći svoja iskustva i ideje.
- **Usmjerena pitanja:**
  - **Trenutne prakse**: Koje trenutne prakse imate za zaštitu djece u svom profesionalnom okruženju?
  - **Priče o uspjehu**: Možete li podijeliti bilo koju uspješnu priču u kojoj su ove prakse rezultirale zaštitom djeteta ili grupe djece?
  - **Izazovi**: Sa kojim ste se izazovima suočili u implementaciji ili održavanju ovih praksi?
  - **Inovativna rješenja**: Da li ste razvili ili usvojili bilo kakve inovativne mogućnosti za rješavanje specifičnih pitanja u vezi zaštite djece?
- **Olakšati diskusiju:**
  - **Otvorena diskusija**: Pozovite učesnike da podijele svoje prakse i iskustva, svaki pojedinačno. Ohrabrite aktivno slušanje i poštovanje prema svakom govorniku.
  - **Interaktivni dijalog**: Promovišite interaktivni dijalog postavljanjem dodatnih pitanja i ohrabrivanjem drugih da odgovore ili dodaju svoja razmišljanja.
  - **Dijeljenje resursa**: Ohrabrite učesnike da dijele sve resurse, alate ili materijale, koje koriste u svojim praksama.

12. RESURSI ZA BEZBJEDNOST NA INTERNETU

Slajd 104

Označavanje efikasnih resursa za sigurnost na internetu.

Slajd 105

U Crnoj Gori postoji nekoliko ključnih organizacija i mehanizama koji pružaju podršku građanima u slučajevima štetnog sadržaja, sajber maltretiranja, prevara i drugih problema na internetu.

1. **Uprava policije Crne Gore**
   - **Odjeljenje za borbu protiv sajber kriminala**: Specijalizovano odjeljenje koje istražuje slučajeve sajber nasilja, zloupotrebe interneta i drugih digitalnih prijetnji. Građani mogu prijaviti probleme direktno putem lokalnih policijskih stanica ili elektronski na zvaničnoj web stranici policije.
2. **Agencija za elektronske komunikacije i poštansku djelatnost (EKIP)**
   - EKIP ima zadatak da nadgleda i osigura bezbjednost komunikacija u digitalnom prostoru, uključujući zaštitu podataka i prijave zloupotreba. EKIP nudi savjete o zaštiti korisnika i mogućnost prijavljivanja problema sa internet provajderima.
3. **Nacionalni CERT (Computer Emergency Response Team)**
   - CERT Crne Gore pruža tehničku podršku i savjetovanje u slučajevima sajber prijetnji, uključujući *phishing*, maliciozni softver i napade na privatnost. Obrađuje tehničke aspekte sigurnosnih problema i može posredovati između građana i internet provajdera.
4. **Ministarstvo prosvjete Crne Gore**
   - **Programi u školama**: Ministarstvo podržava edukativne programe za podizanje svijesti o rizicima na internetu među djecom i mladima.
   - **Prijave u školama**: Nastavnici i pedagozi mogu biti prvi kontakt za prijavljivanje digitalnog nasilja u školskom okruženju.
5. **Zaštitnik ljudskih prava i sloboda (Ombudsman):** Ombudsman se bavi zaštitom prava građana, uključujući zaštitu djece od zlostavljanja na internetu. Ova institucija pruža mehanizme za prijavu kršenja ljudskih prava, uključujući internet nasilje (već je pomenuto "Hrabro sanduče").

https://www.unicef.org/montenegro/zaustavimo-nasilje-onlajn-2016

13. NACIONALNI OKVIR

Slajd 106

Pregled specifičnih nacionalnih mehanizama za prevenciju, prijavljivanje i upućivanje, uz postojeće protokole za svaku kategoriju profesionalaca u slučajevima nasilja nad djecom.

Slajd 107

Standardne operativne procedure (SOP) kao smjernice za sve aktere i relevantna lica zadužena za zaštitu i rad sa djecom žrtvama nasilja i iskorišćavanja u Crnoj Gori.[37]

Na osnovu Studije UN o nasilju nad djecom, Smjernica Savjeta Evrope za nacionalne integrisane strategije za zaštitu djece od nasilja predlažu multidisciplinarni i sistematski nacionalni okvir za prevenciju i odgovor na sve činove nasilja nad djecom.

- ✓ Prevencija nasilja zahtijeva međusektorsku saradnju i koordinaciju. Tu naročito spada koordinacija između organa centralne vlasti, između centralne i lokalne vlasti i između vlade i civilnog društva.
- ✓ Nasilje nad djecom zahtijeva integrisani (sistemski, holistički) pristup. Ovaj pristup omogućava da se različiti faktori (kulturni, psihološki, pedagoški, bihevioralni, fizički, politički, socioekonomski, itd.) tretiraju pomoću zajedničke osnove.
- ✓ Pristup sa više aktera je nezamjenjiv za iskorjenjivanje nasilja nad djecom.
- ✓ Aktivnosti treba da se oslanjaju na međusektorsku saradnju i koordinaciju koja uključuje zdravstveni, obrazovni i socijalni sektor, organe za sprovođenje zakona i pravosudni sistem.

Institucije i organizacije koje su prepoznate kroz SOP:

- ➢ Uprava policije;
- ➢ Pravosudne institucije (krivično odjeljenje sudova, prekršajni sud, vanparnično odjeljenje sudova, građansko odjeljenje sudova);
- ➢ Centri za socijalni rad;
- ➢ Zdravstvene institucije;
- ➢ Obrazovne institucije;
- ➢ OCD koje rade u oblasti nasilja nad djecom i njihovog iskorišćavanja, podrške djeci i porodicama i nasilja u porodici.

37 https://www.zsdzcg.me/sites/zsdzcg.me/files/2024-02/unicef_-_sop_za_medjusektorsku_saradnju_web.pdf

Slajd 108

Standardne operativne procedure obuhvataju:

SOP1: IDENTIFIKACIJA, IZVJEŠTAVANJE, INICIJALNO UPUĆIVANJE I POSTUPANJE PO PRIJAVI;

SOP 2: POČETNA PROCJENA RIZIKA, NEODLOŽNA INTERVENCIJA I PROCJENA POTREBE ZA ZAŠTITOM DJETETA I PORODICE;

SOP 3: ZAŠTITA I POMOĆ DJETETU I PORODICI;

SOP 4: PRAVNA ZAŠTITA I INFORMISANJE DJECE ŽRTAVA NASILJA I/ILI ISKORIŠĆAVANJA.

14. SAŽETAK

Slajd 109 – Sažetak

Pregled svih obuhvaćenih sadržaja i pružanje mogućnosti učesnicima da postave pitanja radi detaljnijih objašnjenja i konsolidacije razumijevanja.

Slajd 110 – Pitanja i kontakt detalji

CNR

www.coe.int

Savjet Evrope je vodeća organizacija za zaštitu ljudskih prava na kontinentu. Obuhvata 46 država članica, uključujući sve članice Evropske unije. Sve države članice Savjeta Evrope potpisale su Evropsku konvenciju o ljudskim pravima, sporazum koji ima za cilj da zaštiti prava čovjeka, demokratiju i pravnu državu. Evropski sud za ljudska prava kontroliše implementaciju Konvencije u državama članicama.

Safe Online

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE