A close up of a logo

Description automatically generated

Predloga za učni načrt

Modul 6

# Načrt lekcije – Modul 6

## Učni rezultati

|  |  |  |  |
| --- | --- | --- | --- |
|  | **ZNANJE** | **SPRETNOSTI** | **STALIŠČA** |
| **Modul 6: ZUNANJE GROŽNJE IN NASTAVITVE ZASEBNOSTI TER STARŠEVSKI NADZOR V DRUŽABNIH MEDIJIH** | Opredelitev koncepta Informacijske zmede (glej Modul 3, Delavnica 1). | Sposobnost prepoznavanja različnih vrst informacij in njihovih oblik (glej Modul 3, Delavnica 1). | Zavedanje pomena medijske pismenosti za zavzemanje aktivne drže pri uporabi in ustvarjanju medijev. |
| Razumevanje, kaj je lažni račun.  Razumevanje razlike med lažnimi računi, ki jih ustvarijo ljudje, in njihovimi nameni ter lažnimi računi, ki jih ustvari programska oprema in njihovimi nameni.  Opredelitev koncepta prevare in njenih ciljev.  Opredelitev glavnih značilnosti prevare. | Sposobnost pojasniti, kaj je lažni račun in kaj je njegov namen (trolanje, satira, prevara, širjenje napačnih informacij; nekatere lažne račune upravljajo roboti in delujejo 24 ur na dan, 7 dni v tednu).  Sposobnost prepoznavanja lažnega računa, s katerim upravlja bot (in njegovih ciljev), lažnega računa, s katerim upravlja človek (in njegovih ciljev), ter bota, ki ne želi biti zamenjan za lažni račun.  Sposobnost pojasniti, kaj je goljufija, in prepoznati poskus goljufije med krmarjenjem v digitalnih okoljih.  Sposobnost prepoznavanja prevare na podlagi več značilnosti prevar (e-poštni naslov, nezaželen ali nepričakovan stik, preveč dobro, da bi bilo resnično, zahteva po osebnih podatkih, zahteva po hitri odločitvi, naključno tekmovanje. | Zavedanje, da lahko lažni računi otežijo navigacijo v digitalnih okoljih in jo naredijo nevarnejšo.  Spoznanje, da imajo različne vrste lažnih računov različne cilje, in zavedanje, kako pomembno je znati razlikovati med njimi.  Spoznanje, da so goljufije po definiciji poskusi prevare s končnim (zlonamernim) ciljem, kot je kraja denarja.  Uporabite kritično razmišljanje in pridobljeno znanje, da boste sebe in svojo družino zaščitili pred prevarami. |
| Opredelitev pojma kraje identitete in seznam načinov, kako se lahko tatovi identitete dokopljejo do osebnih podatkov.  Poznavanje načinov za zaščito osebnih podatkov pred krajo identitete. | Sposobnost razlage pojma kraja identitete in opisati različne načine (kršitve varnosti podatkov, nezaščiteno brskanje, temni splet itd. ), na katere lahko postanemo žrtve kraje identitete.  Uporaba različnih načinov za zaščito osebnih podatkov na spletu (spremljanje kreditnih poročil, nepooblaščenih bančnih transakcij, prenehanje prejemanja računov itd., kontaktiranje pristojnih organov, vzpostavitev opozorila pred goljufijami). | Zavedanje, da je nemogoče v celoti zaščititi svoje spletne podatke, kljub temu pa je na podlagi znanja in pogostega spremljanja računov, mogoče močno zaščititi osebne podatke v digitalnih okoljih.  Zavedanje tveganja, ki je neločljivo povezano s spletnim poslovanjem, in uporaba metode za zaščito osebnih podatkov. |
| Opredelitev pojma gradiva, ki vsebuje spolno zlorabo otrok (znano tudi kot otroška pornografija, vendar se je potrebno uporabi tega izraza izogibati, saj je netočen njegov namen pa je legitimirati izkoriščanje otrok). | Sposobnost razlage pojma CSAM in posledic stika s takšnim gradivom na spletu (nezakonito, zamegljuje "presojo o tem, kaj se šteje za primerno vedenje z otroki ali najstniki" itd). | Zavedanje da je CSAM sodobna različica zlorabe in izkoriščanja otrok na spletu, ki je prav tako v porastu. Prevzemanje osebne odgovornosti in poročanje o gradivu CSAM ter sposobnost pomagati nekomu, ki ima morda neprimerne misli ali se neprimerno obnaša. |
| Opredelitev pojma spletne zlorabe.  Opredelitev pojma kibernetskega ustrahovanja.  Opredelitev pojma drugih oblik spletnih zlorab in načinov njihovega obravnavanja. | Sposobnost razlage in prepoznavanja različnih vrst spletnih zlorab (spletno ustrahovanje, čustvena zloraba, navezovanje stikov, spolna zloraba in izkoriščanje).  Sposobnost razlage in prepoznavanja kibernetskega ustrahovanja v spletnih okoljih.  Sposobnost prepoznavanja več vrst spletnih zlorab in uporabe ukrepov za njihovo odpravljanje (npr. o sekstingu). | Zavedanje, da se zloraba lahko zgodi tudi na spletu, zato jo boste znali prepoznati.  Zavedanje, da je kibernetsko nadlegovanje izraz nadlegovanja, ki se dogaja na spletu (znano tudi kot spletno nadlegovanje ali spletno trpinčenje).  Samozavest pri obveščanju družinskih članov o oblikah zlorab, na katere lahko naletijo ali so jim priča na spletu, ter o načinih, kako se z njimi spopasti. |
| Opredelitev pojma nastavitev zasebnosti.  Poznavanje evropskega pravnega okvira za varstvo osebnih podatkov (Splošna uredba o varstvu podatkov 2016/679). | Sposobnost razlage pojma »nastavitve zasebnosti« in načinov, kako lahko te nastavitve prilagodimo, da zaščitimo svojo zasebnost na spletu (zasebni profil, ne sprejemamo prošenj od naključnih ljudi, ne delimo gesla, objave so vidne samo prijateljem, pregledovanje oznak itd.).  Sposobnost opisati glavne odgovornosti platform družbenih medijev in spletnih podjetij v skladu z uredbo SUVP, pri zbiranju in izmenjavi osebnih podatkov ter splošni komunikaciji s strankami. Izjave o politiki zasebnosti zagotavljajo podrobne informacije o upravljanju osebnih podatkov. | Zavedanje, da večina platform družabnih medijev omogoča prilagajanje spletne izpostavljenosti.  Samozavest pri uporabi varnostnih ukrepov (npr. geslo za dvostopenjsko avtentikacijo) in ukrepov za zaščito zasebnosti v različnih digitalnih okoljih. |
| Opredelitev pojma starševskega nadzora v digitalnem svetu.  Opredelitev vrst starševskega nadzora, ki jih je mogoče uporabiti v družabnih medijih.  Poznavanje večih načinov za uporabo starševskega nadzora na platformah družbenih medijev. | Sposobnost razlage in uporabe starševskega nadzora v različnih (npr. televizijskih, računalniških, video igre itd.) okoljih.  Sposobnost razlage različnih vrst starševskega nadzora (filtri vsebine, nadzor uporabe, orodja za upravljanje in spremljanje uporabe računalnika).  Možnost uporabe starševskega nadzora na več platformah družbenih medijev in poznavanje platform, ki zagotavljajo možnost starševskega nadzora. | Zavedanje, da je starševski nadzor potreben za zagotavljanje otrokom prijazne izkušnje v spletnem svetu.  Priznavanje možnosti staršev, da omejijo izpostavljenost svojih otrok nezaželeni vsebini.  Samozavestna uporaba starševskega nadzora v družbenih medijih, za spodbujanje varne in otrokom prijazne izkušnje. |

Modul 6 obsega učne vsebine za dve 2-urni delavnici. Učni proces modula 6 se prav tako zanaša na 4 ure samostojnega učenja.

# Načrt lekcije

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Vsebina- Opis | Metoda navodil | Trajanje | Zahtevano gradivo/ oprema | Nasveti za izobraževalce, ki naj jih posredujejo udeležencem | Ocenjevanje/vrednotenje | Nadaljnje branje/povezava do virov |
| Uvod | Pozdravite udeležence. V tem času bi se morali med seboj že poznati, vendar lahko ponovno začnete predstavitveni krog, pri čemer najprej predstavite svoje ime in poklic, oziroma vse pomembne informacije o sebi.  Nato predstavite temo tega modula: Zunanje grožnje družbenih medijev.  Udeležence lahko vprašate, na kaj pomislijo ob tej temi, in ključne besede napišete na tablo. | 15 min | Tabla  Pisala | Uvodni trenutek mora biti čim bolj prijazen. Vsi udeleženci morajo imeti občutek, da se bodo imeli lepo, zato se veliko smehljajte! | Ni na voljo | Ni na voljo |
| Modul 6 – Delavnica 1 : Zunanje grožnje | Udeležencem razložite, da se boste osredotočili na štiri glavne teme:   * Informacijska zmeda * Lažni računi * Kraja identitete * Spletna zloraba  1. Informacijska zmeda (20 min)   Prikažite PPT delavnico 1. Po kratkem pregledu teme začnite s testom: Udeležence povprašajte ali se jim zdi prikazan naslov resničen!  Aktivnost zaključite in udeležencem povejte, da imajo, v virih za samostojno učenje, na voljo več informacij o informacijski zmedi.   1. Catfishing (25 min)   Udeležence najprej vprašajte, ali vedo, kaj je catfishing.  Nato predvajajte ta kratek videoposnetek in predstavite koncept:  <https://www.youtube.com/watch?v=JPuaOCiVAh0>  Zdaj ko udeleženci vedo, kaj je catfishing, jim pokažite še en videoposnetek z nasveti za prepoznavanje lažnih spletnih profilov (videoposnetek začnite pri 3:59 in ga ustavite pri 6:32):  <https://www.youtube.com/watch?v=LagwG7bieEA>  Tukaj je seznam orodij, s katerimi lahko prepoznate catfishing:   * Googlovo povratno iskanje slik * Zahtevajte več informacij in nato naredite selfi   Nato začnite razpravo z udeleženci:   * Kakšne cilje imajo te osebe? (kraja identitete, denar, osamljenost, itd.) * Kako preprečiti, da bi vaše bližnje kdo prevaral? * Kaj lahko kot starši storite, da preprečite takšne situacije?   Prikažite PPT »Kako se izognemo takšni osebi«.   1. Kraja identitete (25 min)   Namen catfishinga je lahko kraja identitete. Gre za pogosto zlorabo na spletu.  Udeležencem najprej pokažite ta kratek videoposnetek:  <https://www.youtube.com/watch?v=xnjFb68r29w&ab_channel=GreatLakes>    Da bi se izognili kraji identitete in se varno obnašali na spletu, moramo upoštevati preprosta pravila. Prikažite PPT razdelek »Varno obnašanje na spletu«.  Nato s skupino začnite razpravo o kraji identitete. Skupini razložite, da so tarča teh prevar tudi starejši uporabniki in da to zadeva vse člane družine.  Skupino vprašajte, ali so jih goljufi že kdaj kontaktirali.  Razpravljajte o tehnikah, ki se uporabljajo za krajo podatkov:   * Phising: goljufiva praksa pošiljanja e-poštnih sporočil, ki se izdajajo za sporočila uglednih podjetij, da bi posameznike pripravila do razkritja osebnih podatkov * Pharming: kaznivo dejanje izdelave lažne spletne strani in preusmerjanja uporabnikov nanjo * Vishing: telefoniranje ali puščanje glasovnih sporočil, češ da prihajajo iz uglednih podjetij, da bi posameznike pripravili do razkritja osebnih podatkov * Smishing: pošiljanje besedilnih sporočil, ki naj bi bila od uglednih podjetij, da bi posameznike pripravila do razkritja osebnih podatkov   Skupino prosite, da si med seboj izmenjajo izkušnje o teh praksah in povedo, kako so jih premagali.   1. Spletna zloraba (25 min)   Zdaj boste razpravljali o nočni mori vseh staršev: spletni zlorabi.  Začnite z razdelkom PPT »Spletne zlorabe«.  Po zaslugi predstavitve so udeleženci razumeli, da je aktivno poslušanje ena od glavnih lastnosti staršev. Tako ničesar ne zamudijo in lahko zaznajo težave.  Naslednja aktivnost bo trajala 10 min. Gre za razmišljanje o aktivnem poslušanju.  Udeležence povprašajte, kakšne so po njihovem spretnosti, ki jih poseduje aktivni poslušalec. Odgovore zapisujte na tablo; poskrbite, da se med pogovorom pojavijo naslednji pojmi:   * Nevtralen * Ne obsoja * Potrpežljiv * Verbalna in neverbalna komunikacija * Postavlja vprašanja * Razmišlja o izrečenem * Zahteva pojasnila * Iz povedanega potegne bistvo   **Zaključek**  Na koncu starše vprašajte, kaj so se danes naučili in ali bodo to znanje doma uporabljali. | 20min  10 min | PC/prenosnik  Projektor  PPT delavnica 1  PC/prenosnik  Projektor  Papir in pisalo za zapiske udeležencev  PPT »Kako se izognemo takšni osebi«  PC/prenosnik  Projektor  PPT »Varno obnašanje na spletu«  PC/Projektor  Prenosnik  PPT »Spletna zloraba«  Tabla  Pisala | Ob podpori PPT boste začeli izvajati aktivnost. Udeleženci so se s temo seznanili na delavnici 1 modula 3. | Ni na voljo | Ni na voljo |
| Modul 6 – Delavnica 2 | **Dobrodošli**  Pozdravite udeležence, razložite glavne učne rezultate prejšnje delavnice in jim povejte, da bo to srečanje osredotočeno na nastavitve zasebnosti in starševski nadzor v družabnih medijih.  Delavnico začnite s tem kratkim videoposnetkom:  <https://www.youtube.com/watch?v=UhhYSrUHnao&ab_channel=TechnologyServicesatIllinois>  Ta videoposnetek prikazuje, koliko podatkov je mogoče pridobiti iz preprostih objav v družabnih medijih.  Nato prikažite ta videoposnetek, ki predstavlja evropsko uredbo o osebnih podatkih (SUVP):  <https://www.youtube.com/watch?v=acijNEErf-c&ab_channel=Channel4News>  Z nastavitvami zasebnosti lahko omogočite nadzor nad tem, kdo vidi informacije o vas.  Potem prikažite PPT »Nastavitve zasebnosti«  Poskrbite, da bodo udeleženci lahko postavljali vprašanja.  Prikažite PPT »Starševski nadzor«  Poskrbite, da bodo udeleženci lahko postavljali vprašanja.  Na koncu udeležencem pokažite naslednji videoposnetek, v katerem je predstavljena programska oprema za starševski nadzor:  <https://www.youtube.com/watch?v=9DSAi4q6SmQ&ab_channel=10BestOnes>  Vprašajte jih o njihovem mnenju. Ali menijo, da je takšna programska oprema dobra zamisel? Kaj pa zasebnost otroka? Kako zagotoviti medsebojno zaupanje? | 10 min  5 min  10 min  35 min  30 min  15 min | Ni na voljo  PC/prenosnik  Projektor  PPT delavnica 2  Papir in pisalo za zapiske udeležencev  PC/prenosnik  Projektor  Papir in pisalo za zapiske udeležencev  PC/prenosnik  Projektor  PPT »Nastavitve zasebnosti«  Papir in pisalo za zapiske udeležencev  PC/prenosnik  Projektor  PPT »Starševski nadzor«  Papir in pisalo za zapiske udeležencev  PC/prenosnik  Projektor | Ni na voljo | Ni na voljo | Ni na voljo |
| Zaključek | **Zaključek in vrednotenje modula 6**  Na koncu starše vprašajte, kaj so se danes naučili in ali bodo to znanje uporabljali doma.  Vprašajte jih, ali je modul 6 naslovil njihove potrebe in ali imajo dodatna vprašanja. | 15 min | Tabla  Pisala |  |  |  |

A close up of a map

Description automatically generated

"Podpora Evropske komisije pri pripravi te publikacije ne pomeni, da podpira njeno vsebino, ki odraža izključno stališča avtorjev. Komisija ne more biti odgovorna za kakršno koli uporabo informacij iz te publikacije.”

Številka projekta: 2020-1-AT01-KA204-077958